NUREG/CR-4386
PNL-5544

Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor

Prepared by W. E. Bickford, A. S. Tabatabai

Pacific Northwest Laboratory
Operated by
Battelle Memorial Institute

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-4386
PNL-5544
RG. R1, R4

Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor

Manuscript Completed: October 1985
Date Published: December 1985

Prepared by
W. E. Bickford, A. S. Tabatabai

Pacific Northwest Laboratory
Richland, WA 99352

Prepared for
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B2386

ABSTRACT

Pacific Northwest Laboratory (PNL) performed probabilistic risk analyses to develop estimates of core-melt frequency and public risk associated with control system failures in a Babcock and Wilcox pressurized water reactor. PNL also conducted value/impact analyses of proposed control-system modifications. These analyses were based on failure modes and effects previously identified at Oak Ridge National Laboratory (ORNL). These control system failure modes fall into three main scenarios: 1) overfill of the steam generators, progressing to spillover into the steam lines, 2) ICS hand power failure progressing to steam generator dryout, and 3) ICS automatic power failure progressing to steam generator failure. For each of these modes, two failure sequences were postulated. The results of PNL's probabilistic analysis of failure progression to core damage and value/impact analyses of possible resolutions to prevent these failures are presented in this report.

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

Pacific Northwest Laboratory (PNL) has performed a probabilistic risk assessment (PRA) of control system related failures in light water reactors for the U.S. Nuclear Regulatory Commission (NRC). This work was performed in support of the NRC's Unresolved Safety Issue A-47 program: Safety Implications of Control Systems. This report specifically focuses on control failures in a representative Babcock and Wilcox (B&W) pressurized water reactor (PWR). The PRA was based on PWR failure modes and frequencies developed by Oak Ridge National Laboratory (ORNL) (Clark et al. 1985).

In addition, PNL has performed a value/impact analysis of proposed resolutions to correct control system deficiencies identified by the A-47 program. Value/impact analyses are required by the NRC as input into the regulatory decision process to insure that the need for and consequences of cost-effective regulatory actions are identified (NRC 1983a). Cost/benefit analyses are not the sole or even principal basis for decisions, but they do provide one consideration. The purpose here was to provide merely a screening tool for potential resolutions. A more rigorous value/impact analysis would likley accompany any future specific NRC regulatory actions.

S.1 GENERAL OVERVIEW

The report discusses the following major topics: 1) control system failures identified as being of concern to the A-47 program, 2) safety implications of these failures and potential for progression to core-melt scenarios, 3) calculations of risk probabilities, 4) resolutions to mitigate or eliminate these failures, 5) estimates of potential risk reduction by implementing proposed resolutions, 6) costs of resolutions, and 7) resulting value/impact ratios. These topics will be quickly summarized here, followed by a more detailed summary of the technical analysis and results.

Control Failures of Interest

The A-47 program focused only on 1) those control failures that could initiate a more severe plant response than previously predicted in design basis accidents, or 2) failures that could cause plant conditions to exceed operating technical specifications. Using the Oconee 1 plant as a representative B&W PWR, ORNL identified three failure scenarios involving overfill of the steam generators (SGs), and two involving possible electric circuit power failures leading to steam generator dryout.

Safety Implications

For the first failure scenario, overfill of the steam generators is initiated by failures in the main feedwater system (valves and control logic) plus an undetected failure in the high-water level trip circuit. If not terminated by the operator, this could lead to water pouring into the steam lines, possibly resulting in steam line damage including major steam line

failure. A large uncertainty currently exists concerning this potential, so a high probability of main steam line break (MSLB) was assumed, given spillover of water into the steam lines. A main steam line break in itself is not a significant contributor to core melting scenarios in a PWR, given the isolation of the break from the primary coolant piping. The excessive cooldown, however, could contribute to potential core damage, and introduce the potential for steam generator tube ruptures (SGTRs) given the rapid loss of pressure on the steam side of the tubes. The SGTR in turn could cause a loss of coolant accident (LOCA), which is a real initiator of core overheating and melting if safety injection of water fails.

The two steam generator dryout scenarios likewise create conditions of inadequate core cooling which can lead to core melting if not prevented via reestablished SG cooling or with safety injection of water into the reactor vessel.

Finally, a transient shutdown in the plant can demand safety systems which in turn have the potential for failure. The overfill event identified by ORNL was thus also examined as a potential transient initiator without the power conversion system available for decay heat removal.

Probabilistic Risk Assessment

Event trees were developed for the above scenarios to estimate the probability of system failures causing the progression of the accident to core damage or core-melt. This provided a conditional probability of core damage given the initiating event. When multiplied by the frequency of the initiating event, the frequency of core damage and core melt was obtained. The considerations for MSLB by ORNL (ORNL 1982) and the Institute for Nuclear Power Operations (INPO 1982) were used to evaluate the potential for core damage given an MSLB. The results of the NRC steam generator tube integrity program (NRC 1985) were used to estimate the probability for SGTR given a MSLB. Core melting sequences for SGTR were also based on this program's results and on the probabilistic risk assessments performed for the Oconee plant (EPRI 1984, Kolb et al. 1981). Recovery from the dryout scenarios relied entirely on operator recovery of feedwater to the SGs, or failing that, operator use of the high pressure injection system to cool the core.

ORNL estimates (Clark et al. 1985) of initiating frequency for the three failure scenarios were used, combined with a PNL "best engineering" estimate of the probability of subsequent protective system failure. Based on ORNL initiating frequencies of 6.0E-03/py, 9.0E-03/py, and 9.0E-03/py for the overfill and two dryout scenarios respectively, PNL estimated the core-melt frequencies at 9.6E-06/py, 9.0E-06/py, and 2.8E-06/py respectively, for a total core-melt frequency of 2.14E-05/py.

Representative radioactive release categories for the core-melt scenarios were chosen based on a review of the PRAs, with associated public doses as proposed for the NRC for evaluating safety issues (Heaberlin et al. 1983). The risk estimated then was 45.8, 24.4, and 7.7 man-rem/py for the three scenarios, respectively.

When compared with the risk estimated for other nuclear safety issues (NRC 1983b), these core-melt frequency and risk estimates are significant. When the NRC prioritizes efforts to resolve safety issues, a further examination of the costs associated with possible resolutions to mitigate these failures would be justified. The results of the preliminary value/impact assessment of these modifications are presented below.

Risk Reduction/Cost/Value-Impact

A number of modifications were examined to correct the modes initiating the three failure scenarios. These included isolation valves for the feedwater system to block overfill and increased maintenance inspections or modifications to the relay logic to help prevent the failure of the high water level trip circuit. Automatic actuation of emergency feedwater on low steam generator levels was also examined.

The final conclusion was that given the significant risk estimates involved, all of these modifications appear to be feasible and cost-effective. Again, this value/impact information provides only one input to the regulatory decision process. It is expected to be subject to further scrutiny by the NRC, ORNL, and by affected utilities, all of which can bring additional insight and perspective to these results.

Finally, it should be noted that control system failures similar to those postulated in this report have occurred in operating PWRs. However, there has been no known progression of such failures to core damage and subsequent release of radioactive material. The accident sequences developed in this report are therefore speculative and subject to all the uncertainties and limitations surrounding the use of probabilistic risk assessment for predicting nuclear safety.

S.2 TECHNICAL OVERVIEW

The potential control system failures identified by ORNL again deal primarily with overfill of the steam generator with the potential for water entering the steam lines, and two possible scenarios leading to dryout of the steam generator. The technical details of these analyses are described in depth in the following subsections. Each of the three control system failure scenarios is described, followed by a discussion of some of the limitations and areas of conservatism invoved in the analyses.

Failure Scenario 1--Steam Generator Overfill

The steam generator overfill scenario deals with the potential for undetected failures in the high SG water level main feedwater (MFW) trip function. The risk associated with this scenario was examined by considering several possible accident sequences: 1) a transient shutdown with the power conversion system unavailable because of degrading conditions in the secondary side, 2) SG overfill progressing to spillover and main steam line break (MSLB), and 3) MSLB progressing to SGTR.

The resulting risk estimates are given in Table S.1. As can be seen, risk estimated for the MSLB progressing to SGTR is dominant for this scenario. The assumption was made that, given main steam line damage, there is a 50 percent probability that an MSLB would occur outside of the reactor building. This would mean that water released from the break would not be collected in building sumps for recirculation. The ability to isolate the affected SG can play an important role in recovery from a SGTR; however, unlike many B&W reactors, the Oconee plant does not have any main steam isolation valves (MSIVs). A Category 2 release (NRC 1975) was then assumed for public risk. This type of release involves an early core-melt with failure of the containment sprays, which is consistent with exhaustion of recirculation inventories.

The estimated potential for core-melt in a PWR, given SGTR, typically depends on 1) the assumed potential for MSLB given spillover, and 2) the break location if an SGTR occurs. For this analysis, effective probabilities of MSLB, and SGTR given MSLB were established at 0.95 and 0.034, respectively. Break location, however, is not as important in Oconee due to the lack of MSIVs when compared to the H. B. Robinson plant examined earlier for the A-47 program (Bickford and Tabatabai 1985b).

The design modifications proposed to reduce the frequency failures described in this scenario focus on the potential for undetected failures in the high level MFW trip function. ORNL assumed this failure probability to be fairly high because of the annual inspection frequency. Changing to a monthly inspection frequency was assumed to reduce the failure potential by a factor of two. This testing frequency would be possible for most components (e.g., comparative signal readings from transmitters, etc.), however, the trip relays themselves are in series and thus do not lend themselves to online testing.

The ORNL suggestion to add an additional FPTX relay to make the trip relay circuits associated with each generator parallel in configuration was then examined. A factor of 10 reduction in the failure frequency was assumed if modifications actually make it possible to test the generator trip circuits alternately during operation. The man-rem reduction associated with the monthly testing of this new trip circuit was estimated to be 1050 man-rem over 30 years. The costs associated with the modification and testing were estimated to be approximately $200,000, giving a value/impact ratio of 5.3 man-rem/$1,000.

A second proposed modification involves the addition of a new trip circuit for the feedwater block valves. This appears to be a very viable alternative to terminating feedwater flow. If driven from independent level transmitter signals, such as from startup range transmitters, the independent trip would effectively eliminate approximately 97 percent of the risk represented by overfill. The value/impact analysis indicates that if costs for such a modification were kept under approximately $250,000, the value/impact ratio would be more favorable for the monthly testing modifications, in addition to being more effective in reducing the frequency of overfills.

TABLE S.1. Summary of ORNL and PNL Estimates of Accident Initiator Frequencies, Core-melt Frequencies, and Public Risk for the B&W Oconee PWR

	ORNL [a] Accident Initiating Frequency Best Estimate (/py)	PNL Core-Melt Frequency Best Estimate (/py)	PNL Public Risk Best Estimate (man-rem/py)
Sequence Initiator			
Overfill & High Trip	6.0E-03		
Failure:			
T2 Transient Shutdown		6.88E-08	1.86E-01
MSLB		6.27E-08	1.71E-01
SGTR		9.45E-06	4.54E+01
		9.58E-06	4.58E+01
ICS Hand Power Failure with SG Dryout	9.0E-03	9.00E-06	2.44E+01
ICS Auto Power Failure:	9.0E-03		
SG Dryout		2.70E-06	7.31E+0
T2 Transient Shutdown		0	0
MSLB		1.16E-09	3.14E-03
SGTR		8.77E-08	4.21E-01
		2.79E-06	7.73E+0
TOTAL		2.14E-05	7.79E+01

(a) ORNL estimates of initiating frequencies include operator error

No modifications to a 2-out-of-3 or 2-out-of-4 trip logic were postulated by ORNL. At the request of the NRC, a number of logic modifications were evaluated and found to have risk reductions similar to those postulated for improved reliability of the high-level trip function. However, the value/impact ratio of such modifications is highly sensitive to the cost of additional level transmitters and associated hardware. Given the different control functions of the level transmitters and high trip in the B&W design, and given the high degree of uncertainty in the cost of modifications, changes in the level transmitters appear less beneficial. Similar risk reductions would be possible through improving testability of the high-level trip function with much less uncertainty in the associated costs.

Failure Scenarios 2 and 3--Steam Generator Dryout

The remaining failure scenarios identified by ORNL involve steam generator dryout; these scenarios are described below.

Loss of ICS Hand Power

The loss of the ICS hand power circuit was found to present the potential for steam generator dryout if the operator failed to reestablish feedwater flow within 30 minutes or HPI flow within 60 minutes following loss of this power supply. Several modifications were developed which could potentially reduce the frequency of automatically progressing to dryout. These modifications included emergency feedwater (EFW) actuation on low SG level, MFW trip on loss of hand power which would initiate EFW flow, a higher minimum runback setpoint on the MFW to prevent the zero MFW flow, and rewiring the loss-of-voltage signal to the MFW pump controller to represent a 50 percent setting. This last modification is apparently used in other B&W plants.

The potential risk reduction possible by reducing the initiating frequency a factor of 10 was estimated to be 659 man-rem over 30 years. No costs for the above modifications were estimated. It was pointed out, however, that the cost of the above modifications was thought to easily be under $659,000, giving value/impact ratios in excess of 1 man-rem/$1000.

Loss of Auto Power

The loss of automatic power was initially thought to leave the plant in an unstable equilibrium, allowing the operator time to manually control the reactor before the development of an instability and subsequent trip. Oconee personnel indicated that this is how they would respond to such a failure. However, ORNL studies have indicated that no annunciators are associated directly with the H1 circuit which serves the majority of feedwater components, and that no emergency procedures exist. As a result, an event tree assuming eventual reactor trip without prior operator awareness of the failure was assumed. The operator would then be required to reestablish feedwater flow as with the above scenario.

Annunciated power failure and proper emergency procedures were estimated to provide a 155 man-rem risk reduction over 30 years by lowering operator error. The costs for implementing such modifications were estimated to be minimal, giving a value/impact ratio of 2 man-rem/$1000.

Initiation of EFW on Low Level

A final modification involving automatic initiation of EFW on low level signals from the SG level transmitters was examined. This modification would effectively eliminate the two scenarios involving loss of ICS power that requires operator action to reestablish feedwater before generator dryout occurs. The modification only provides an additional initiation signal and does not appear to degrade or jeopardize the current operating mode of the EFW.

Examination by ORNL indicates that this modification does not require a cross-tie between a safety and non-safety grade system or require a full safety

upgrade of the level transmitting equipment. Two 1E "startup range" level signals per SG are currently used for EFW valve control 1 and could be used for initiation.

Results

Table S.1 summarizes the total estimated core-melt frequency and public risk (2.14E-05/py and 78 man-rem/py, respectively) represented by all three scenarios. These values compare to the overall core-melt frequency for the Oconee plant of 8.20E-05/py, with a public risk of 207 man-rem/py. The overfill scenario leading to spillover and the dryout scenarios thus represent a significant fraction (20 percent) of this risk.

Table S.2 presents the results of the value/impact analysis, examining the possible cost and risk reduction associated with design modifications. Note that for several modifications, no direct cost estimate is made. Rather, the maximum costs that will keep the resulting value/impact ratio at or above the 1 man-rem/$1000 figure of merit are indicated.

All modifications examined appeared capable of being justified based on the value/impact ratio. The failure modes identified by ORNL appear to be readily amenable to correction without extensive modification; thus the costs estimated are not restrictive in any sense.

Modifications to Trip Logic

This analysis partially examined the possible reduction in high-level trip failure probability associated with installing a more complex high-level trip logic for the main feedwater pumps. In the PNL examination of the GE BWR and Westinghouse PWR, the installation of a 2-out-of-4 trip logic did not appear to be favorable (Bickford and Tabatabai 1985a and b). However, in the Oconee B&W PWR plant, the output from the level transmitters is not used as a level control signal to maintain an exact steam generator water level as in the case of the GE and Westinghouse plants. Instead, the water level in the B&W design varies within a broad operating range. Conditions are maintained within this range to give the proper degree of steam superheat at the generator output rather than to maintain a set water height. The normal configuration is then a 2-out-of-2 logic on each generator rather than the 2-out-of-3 logic seen on the Browns Ferry and H. B. Robinson plants.

The GE and Westinghouse designs combine the feedwater level control and trip functions with the level transmitters. A failure that could both fail the high trip and drive the feedwater increase thus becomes the dominant failure mechanism. Modifications proposed address the level transmitter failure modes and logic. Because these functions are separate in the B&W design, the dominant failure identified by ORNL is an undetected failure of the high trip. As such, corrective actions should be directed at this failure specifically for the B&W plant.

TABLE S.2. Summary of the Value/Impact Analysis for the Oconee B&W Plant

Proposed Fix	Scenario Affected	Estimated Cost, $1000	Estimated Risk Reduction (man-rem)	Value/Impact Ratio (man-rem/$1000)
Monthly Testing	Overfill & undetected high trip failure	88	4.53E+02	5.2
Monthly Testing Plus Parallel FTPX Relay	Same as above	200	1.05E+03	5.3
Feedwater Block Valve Trip Circuit		83	1.34E+03	16.2
Modified Trip Logic (See Note 1)				
1. 1-out-of-1, 1 FTPX with two spurious trips in 30 years		624	4.53E+02	0.73
2. 1-out-of-2, 1 FTPX with two spurious trips in 30 years		612	8.99E+02	1.47
3. 2-out-of-3, 1 FTPX		300.16	8.86E+02	3.0
4. 1-out-of-2, 2 FTPX with two spurious trips in 30 years		636.0	1.15E+03	1.8
5. 2-out-of-3, 1 FTPX per LT		312	1.15E+03	3.7
6. 2-out-of-4, 1 FTPX		600	9.07E+02	1.5
7. 2-out-of-4, 2 FTPX		612	1.17E+03	1.9
MFW Trip on Loss of ICS Hand Power	ICS Hand Power Failure with SG dryout	-	-	-
Higher Minimum MFW Setpoint		-	-	-

TABLE S.2 (Continued)

Proposed Fix	Scenario Affected	Estimated Cost, $1000	Estimated Risk Reduction (man-rem)	V/I Ratio (man-rem/$1000)
MFW Default to 50% output on 0 Voltage (see Note 2)		- 6.59E+05	- 6.59E+02	- 1.0
Annunciation of Auto Power Failure and Emergency Procedures	Auto Power Failure	7.36E+04	1.55E+02	2.04
EFW Initiation on Low SG Level	ICS Power Failures	1.0E+05	8.68E+02	8.68

Note 1: Value/impact ratios for modifications to trip logic would be lowered by approximately a factor of 10 if implemented after other modifications.

Note 2: Cost of any or all of above can be less than $659,000 and still give a value/impact ratio equal to or greater than 1 man-rem/$1000.

Note 3: Cost of implementing the EFW initiation function can be as high as $868,000 or approximately $1,000,000 per plant and still give a value/impact ratio on the order of 1 man-rem/$1000.

Although the 1-out-of-1 type logics for the high-water level MFW trip function are theoretically superior to more complicated configurations in preventing spillover, the possible costs associated with spurious trips make such simple configurations undesirable. The realistic options for the A-47 program are the 2-out-of-3 and 2-out-of-4 options, with one FPTX relay or with two FTPX relays in parallel. All of these options significantly reduce the trip failure probability to a value nearly equal to that of the MFW valves themselves (0.007/demand). As a result the value/impact ratios associated with these configurations are relatively insensitive to risk reduction but highly dependent on cost. As expected, those options that require the fewest hardware additions appear to perform best from a value/impact standpoint (i.e., the 2-out-of-3 with 1 FTPX relay). The 2-out-of-4 logic is predicted to perform slightly better in preventing overfeeds and spillovers, as was the case in the PNL studies of the

GE and Westinghouse plants. The cost, however, can be significantly more than the other options if additional penetrations are required. The configuration also makes it easier to design online testing procedures more in keeping with safety grade component requirements.

However, the risk reduction and value/impact ratios estimated for such hardware changes are comparable to those for monthly testing alone. The monthly testing alone is estimated to significantly reduce that portion of the MFW high-level trip failure probability due to instrument failure (0.047/demand with 85 percent due to transmitter or relay failures and 15 percent due to MFW valve failures). Any modifications to the trip configuration or logic after implementing such testing would be subject to some diminishing returns in risk reduction, acting on only approximately 8.5 percent instead of 85 percent of the original high trip failure probability. As a result, if configuration changes are made after monthly testing has been implemented, the value/impact ratios predicted for hardware changes would be reduced by approximately a factor of 10. The NRC must then decide if the current system is inadequate, and to what level improvements will be required.

Limitations and Real-World Considerations

Additional uncertainties in calculating feedwater control reliability further contribute to a solution that favors monthly testing over hardware changes. It must be pointed out that any comparison between different level control and high level trips and other modifications is highly conditional on a number of factors, including basic hardware and reliability as well as operator and plant response to system failures. Variables can include plant-specific differences in and compensations for a number of factors, including:

- type of level control (three element, one element)
- power supplies
- backup or alternate level displays
- instrument line plumbing configuration
- controlling level display
- controlling level record
- annunciators and alarms
- operator training and procedures
- maintenance, general age and state of equipment.

The indications are that real world considerations could easily overshadow theoretical calculations, particularly for level control instrumentation where testability often carries more weight than calculated reliability. As pointed out in previous PNL reports, uncertainties could include hydraulic shocks, which occur at different rates in separate instrument lines making some failure combinations of sensors more likely, or common mode failures of instruments due to improper maintenance. The data currently available on component failure rates are not specific enough about failure cause (i.e., shocks, faulty maintenance, etc.) and failure mode (i.e., inoperable low scale, drift low, etc.) to support specific recommendations based on theoretical calculations for level transmitters.

Areas of Likely Conservatism

Again, a "best engineering estimate" of failure probabilites was used whenever possible in the analysis of core-melt and risk for the control system failure modes identified. However, some uncertainty does exist in several factors, and a high failure probability is used. This would in turn weight the estimated core-melt frequency and public risk to higher values. The areas of probable conservatism include:

1) Operator Error. The probability estimated by ORNL for failure of the operator to diagnose and terminate the scenarios ranged from 0.7 for scenarios with misleading or conflicting information or rapid progression (i.e., overfill in several minutes) to 0.1 for scenarios with slow progression and non-conflicting information and alarms. The high value of 0.7 was assumed for this analysis. An average failure probability may be lower, particularly in plants with simulator programs stressing proper diagnosis of failures.

2) Steam Line Break. Main steam line breaks (MSLBs) in PWRs were not assumed to be associated with core-melt in an NRC (1975) study. More recent studies have equated MSLB with core damage which is thought to be equal to or less severe than a core-melt in terms of radionuclide release by up to a factor of 30. This study equated the consequences of MSLB with core-melt.

   The probability of MSLB given spillover into the steamlines at power was assumed to be 1.0, decreasing to 0.5 for spillover after shutdown. Although several spillover events have occurred to date in U.S. commercial plants resulting in support damage, no steam line failures have occurred. The Oconee plant has no MSIVs, making break isolation impossible. Other B&W plants, however, do have MSIVs, making break location important in other plants.

   The MSLB was further assumed to have a significant probability of inducing an SGTR, with the combination of SGTR and unisolatable MSLB leading with high probability to core-melt in a PWR. This high probability of failure to recover is due primarily to depletion of the reactor water storage tank (RWST) water supply before depressurization of the reactor can be achieved. This gives no credit to other operator-initiated means of maintaining the water supply.

   Further information on the probability of MSLB for various overfill scenarios and the break location for other B&W plants could significantly reduce the risk associated with these scenarios, as would a more realistic analysis of operator initiated actions to restore water supplies and avoid core-melt.

3) Transient Shutdown. The initiating event would cause a transient-induced plant shutdown, with loss of the power conversion system (PCS) representing a serious precursor to core-melt in PWRs. A high probability of loss of the PCS given spillover was assumed in this study, but it contributed insignificantly to risk due to the low initiating frequency.

4) Release Categories. The WASH-1400 (NRC 1975) release categories most representative of the core-melt scenarios in this analysis were used to estimate risk. The risk per event values used were from the Value-Impact Handbook (NUGER/CR-3568) (Heaberlin et al. 1983). Ongoing evaluation of the source terms for various core-melt scenarios indicates that the WASH-1400 release categories may overestimate risk by up to several orders of magnitude. This would result in lower risks being attributed to these scenarios.

5) Costs. Estimates of the costs associated with modifications in nuclear plants typically underestimate the final costs, even when accompanied by an extensive engineering cost study. Higher than expected costs would further lower the value/impact ratios estimated here for proposed modifications.

As a result of these uncertainties and their possible negative impacts on operational reliability and the unique dynamic control features of the B&W design, implementing monthly testing to improve reliability appears to be preferable at this time. This recommendation should be regarded as preliminary, and should be subjected to detailed evaluation if plant modifications are considered.

1.0 INTRODUCTION

The purpose of this report is to estimate the potential frequency of core-melt and public risk associated with control system failures in Babcock and Wilcox (B&W) pressurized water reactors (PWRs), and to evaluate the value/impact ratios associated with modifications proposed to mitigate these failures. These failure modes were identified by the Oak Ridge National Laboratory (ORNL) in their examination of the Duke Power Company Oconee-1 Nuclear Power Plant (Clark et al. 1985). This plant was also the subject of a Reactor Safety Study Methodology Application Program (RSSMAP) probabilistic risk assessment (PRA) (Kolb et al. 1981). The Oconee Unit 3 was also the subject of a PRA (Lewis et al. 1984). These studies will be used in the evaluation of core-melt and public risk presented here.

The ORNL investigation identified three major failure modes impacting reactor safety as a result of control system failures:

1. Steam generator (SG) overfilling with undetected failure of MFW high level trip

2. Loss of ICS hand power

3. Loss of ICS auto power.

For each of these major failure modes, specific failure sequences in the control system have been identified and will be discussed in the following chapters.

This work is a direct extension of PNL's assessment of the potential core-melt frequency and public risk associated with control system failures in GE BWRs and Westinghouse PWRs (Bickford and Tabatabai 1985a and b). These studies were based on failure mechanisms identified by the Idaho National Engineering Laboratory (INEL) for a General Electric (GE) plant (Bruske et al. 1985) and a Westinghouse plant (Ransom et al. 1985). The approach used in these two studies is further developed here for the B&W PWR.

2.0 STEAM GENERATOR OVERFILL

The ORNL report (Clark et al. 1985) identified control system failures that could lead to steam generator overfill. ORNL indicated that overfill in a PWR could

1. produce secondary side damage that might compromise safety equipment or cause a series of events which might have primary side effects, including radiological leakage

2. cause densification of primary coolant, reducing pressure, possibly causing loss of pressurizer control, and possibly vapor-locking the primary flow path, and possibly introducing excess reactivity from cold flow

3. provide excess cooling that might in some cases contribute to pressurized thermal shock (PTS).

The purpose here is to attempt to quantify the safety significance of overfill. This event can then represent the initiation of a transient requiring plant shutdown or response of the engineered safety features. The first manifestation of system damage in the overfill scenario is the potential for main turbine damage and turbine trip, which in itself is not a serious challenge to plant systems. However, the potential for excessive moisture carry-over and even spillover does introduce the potential for water hammer and main steam line break (MSLB).

The WASH-1400 study (NRC 1975) considered the consequences that could follow from ruptures on the secondary side of a steam generator for a Westinghouse PWR (Surry). Some 30 possible accident sequences were identified, all ending in either a rapid cooldown transient or a loss-of-coolant accident (LOCA). It was concluded that the transients induced by steam generator failures did not lead to core-melt but could release radionuclides from the fuel-clad gap due to fuel damage. The end result was that SGTR was not identified as an important factor in the risks due to transient events.

However, to be conservative, the excessive cooldown transient is modeled with an appropriate event tree for steam line break. The potential for core damage as a result of MSLB will then be given. In addition, the potential for inducing an SGTR or multiple ruptures will be considered.

An examination of the potential for PTS in the Westinghouse plant, based on the parameters generated by INEL (Ransom et al. 1985) for the postulated failure scenarios, indicated that thermal shock generated could exceed technical specification limits. However, based on preliminary data from the NRC PTS program, the probability of vessel failure is currently estimated to be less than 1E-06.

A discussion of the failure initiators identified by ORNL is given below, followed by a consideration of progression of the accident to MSLB or SGTR and core-melt.

2.1 STEAM GENERATOR OVERFILL

The ORNL analysis of the Oconee-1 main feedwater (MFW) control system indicates that steam generator (SG) high water level control is maintained via both throttling of the feedwater control valve and a high level trip of the main MFW pumps. The integrated control system (ICS) uses two level transmitters per SG. One of the level signals generated is selected and used to limit the feedwater demand signal, with SG water input controlled through the feedwater control valve. In addition, both SG signals per SG are fed to ICS bi-stables which form an array to provide a high SG water level trip signal for the main feedwater pumps. A non-ICS FTPX relay is used for this purpose. The latter relay receives a signal to close and trip the MFW pumps at 359 inches of water. The MFW cannot overfill a steam generator (above the 359 inch level) unless both high level protection features are defeated and an overfeed mechanism is initiated that is not controlled by cross limits or any of the other compensatory features of the ICS.

Overfill of the Oconee steam generators thus requires failures that initiate an overfeed, failure of the MWF trip signal, and failure of the operator to isolate the feedwater flow.

Note that the auxiliary feedwater system (AFW) is not subject to the high level protection features. Therefore, once the system is on AFW, fewer control system failures are required to bring on SG overfill. However, there are mitigating factors. First, there must have been a prior failure or unusual circumstance to bring on the AFW. The other factor is that the AFW pumps water much more slowly than the MFW with a fully open or nearly fully open control valve. Hence, in the AFW case, there is more time for intervention.

The following initiating failures have been identified by ORNL to bring on SG overfill:

A) Failures that place both the level MFW pump trip and the high level control valve closure in a failed state. Since both of these systems depend on the same level detection equipment, a failure there would affect both systems equivalently.

B) Failures that place the high level MFW pump trip in an undetected failed state.

C) Failures that block the high level MFW control valve closure and also initiate steam generator overfeed.

D) Failure that may initiate fast overfeed by the MFW.

E) Failures that would cause MFW overfeed at a relatively low rate; these failures would provide more time for operator intervention.

F) A single failure causing relatively slow overfill of the steam generator, e.g., a sufficient leak in a selected pressure tap or the connecting pipe from that tap, or the packing of the blocking valves on which the connecting pipe terminates.

ORNL made the following conclusions regarding the above failure initiators:

- Type A and B failures do not cause SG overfeed but block some or all of the high-level protection.
- Type C failure, taken alone, should cause a rapid filling of the steam generator to the 359-inch level followed by MFW pump, reactor, and turbine trip and initiation of AFW. Type D failure, taken alone, may be controlled by the ICS.
- One Type F single failure was identified.

A more detailed discussion of these failure initiators is provided in the ORNL report (Clark et al. 1985).

Initiating Event Frequency

The important overfill scenario that may progress to actual spillover of water into the steam lines is the Type B failure, where a failure of the high-level MFW pump trip is undetected, followed by an ICS failure which causes a feedwater increase. The failures contributing to this undetected failure state are given below, with ORNL's estimates of the potential for failure on demand based on an annual testing interval. ORNL further assumed that 50 percent of the annual failures would be detected and repaired during this period. The estimated failure probabilities are listed below:

a) either MFW pump intercept valve fails	0.001/demand
b) either MFW pump trip solenoid valve fails	0.006/demand
c) MFW pump trip relay FTPX fails	0.009/demand
d) either SG operate range level transmitter fails	0.004/demand
e) either multiplication module fails	0.018/demand
f) either signal monitor module fails	0.007/demand
g) either signal generator module fails	0.002/demand

This totals to an estimated failure-on-demand probability of 0.047 for the undetected failed state of the high level trip function.

The initiating frequency for feedwater increase during this period of undetected high trip failure was placed at 0.144/py. This was coupled with a failure of the MFW trip on demand of 0.047.

ORNL estimated the potential for an operator to fail to terminate the overfeed to range from 0.7 to 0.1, depending on the rate of overfeed. This range is consistent with previous PNL estimates of operator error ranging from 0.1 to 0.5 for overfills in the GE and Westinghouse plants.

Based on these data, PNL estimates the range in frequency to be (0.144/py)(0.047)(0.7) = 4.74E-03/py to (0.144/py)(0.047)(0.1) = 6.77E-04/py, or 0.005 to 0.0007/py to one significant figure, depending on the operator error used. Overfill frequency was estimated in the range of 0.006 to 0.001/py by ORNL, citing a more rigorous reduction of the fault trees.

The approach used by PNL in previous studies of overfill in the Browns Ferry GE BWR and H. B. Robinson Westinghouse PWR (Bickford and Tabatabai 1985a and b) was to use a best and upper estimate of the overfill initiation frequency as provided by INEL, coupled with a single conservative estimate of the operator failure probability. To be consistent with this approach, ORNL's higher estimate of 0.7 for operator failure will be used here, giving a best estimate for overfill of 0.0006/py. ORNL did not make an upper estimate of the initiating frequency for overfeed. Rather, the uncertainty was reflected in the severity of the overfeed and likely time for operator response. The 0.7 factor could then be interpreted as an upper bound estimate of the probability of operator error given overfeed.

2.2 ACCIDENT PROGRESSION ANALYSIS FOR SG OVERFILL

For this evaluation, accident progressions to steam line break and possible SGTR are the scenarios of interest for progression to core-melt. The potential for pressurized thermal shock (PTS) leading to vessel rupture should also be considered. This will require thermal hydraulic simulations of excessive cooldown in the B&W design given MSLB. ORNL does indicate, however, that probability estimates of MSLB progressing to PTS as calculated by the PTS program did not show it to be a significant contributor to risk. This sequence will, therefore, be assumed to play an insignificant role in progressing to core-melt, as was the case with the Westinghouse PWR. This assumption can be updated as more information is made available from the PTS program.

Main Steam Line Break (MSLB)

The NRC (1975) analysis of the Surry plant concluded that steam line breaks are not a viable pathway to core-melt. However, the ORNL Precursor Study (Minarick and Kukielka 1982) and the updated INPO Precursor Study (INPO 1982) did include MSLB-initiated event trees leading to core damage, and these will be used here as a conservative estimate to the contribution to core-melt from this type of failure.

As discussed in previous PNL examinations of overfill in the GE BWR and Westinghouse PWR, the probability of MSLB given spillover has been conservatively valued at 1.0 given spillover at rated power, and 0.5 for spillover after main turbine failure and plant trip. The latter figure would include the potential for continued water buildup after SCRAM and pipe failure due to excessive static load. A 0.1 probability of turbine trip was assumed, giving a net probability of (1.0)(0.9) + (0.5)(0.1) = 0.95 for MSLB. A lower probability of 0.5 was proposed for spillover at low power.

The ORNL analysis identified specific overfill scenarios that maximized the overfill aspect of the control system failure in a PWR. Using the

assumptions outlined above, a probability of 0.95 for MSLB given overfill will again be used here. The frequency of MSLB for this scenario is then estimated to be (0.006/py)(0.95) = 5.70E-03/py. The ORNL evaluation indicated that protective turbine trips do in fact exist. A transient-induced shutdown is thus more likely, and will be discussed further below.

Accident Progression to Core-Melt Given Transient or MSLB

The MSLB was not considered a dominant contributor to core-melt in the ORNL study. For this analysis, the results of the ORNL Precursor study as updated by INPO will be used. The resulting event tree for core damage given MSLB in a PWR is given in Figure 2.1. The predicted probability of core damage given MSLB is then estimated at 1.1E-05. The failures involved in the overfill scenario are not thought to impact the response of the engineered safety systems in any fashion. The predicted frequency of core damage due to MSLB is then estimated at (5.70E-03/py)(1.1E-05) = 6.27E-08/py. A further reduction by approximately one order of magnitude is typically used to convert to the probability of core-melt, but this estimate will be used here as a conservative estimate of core-melt.

T2 Transient Shutdown

As mentioned previously, the potential for main turbine trip before the point of spillover exists. Degrading steam quality will introduce excessive moisture in the steam flow to the main turbine. Being highly sensitive to such moisture, this could induce a turbine failure and reactor SCRAM. This main turbine damage represents a T2 transient in the Oconee PRA, this being a loss of the power conversion system caused by other than loss of offsite power. The T2 transient above represents a significant initiator to core-melt regardless of the potential for MSLB. The frequency of T2 transients in the Oconee study is put at 3/py. The total contribution from all T2 sequences in the Oconee PRA add up to a predicted core-melt frequency of 3.44E-05/py out of a total plant core-melt frequency of 8.2E-05/py. In this scenario, the sequence of interest is one in which the operator again fails to terminate the overfeed, and where turbine failure occurs before MSLB. Transients with the PLS available contribute a core-melt frequency of 1.1E-06/yr with an initiating frequency of 4/yr. The T2 transient thus represents the more serious core-melt initiator.

Again, in the above analysis the probability of turbine failure was weighted toward continued operation on the theory that this would be more likely to create the conditions for the presumably more serious water hammer and MSLB. The probability of continued operation was then put at 0.9, with 0.1 probability of failure. The 0.1 factor should be used given the assumption made above. In reality, turbine trip due to failure or an out-of-balance signal may be much more likely, especially given spillover of water into the steam lines.

In this case the initiation frequency is put at 0.006/py, assuming the 0.7 operator error represents the failure to terminate the overfill before turbine failure. Although no mechanisms for loss of the PCS have specifically been identified, the potential exists for loss of the feedwater or decay heat sink

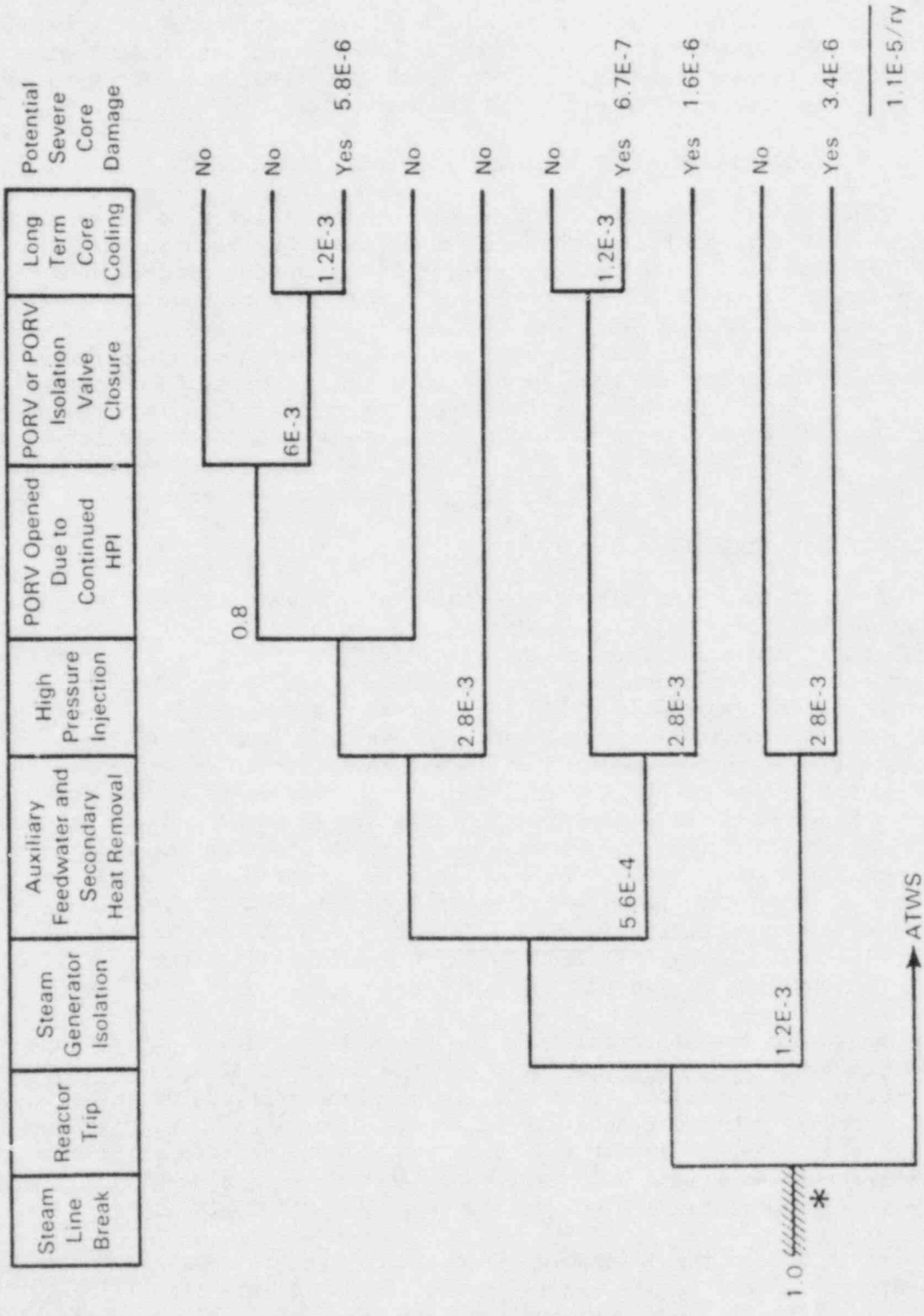

FIGURE 2.1. INPO Event Tree for Propagation of MSLB to Core Damage

being aggravated by the transient. The probability of loss of the PCS is not certain if this is assumed to be 1.0, this will give a net frequency of a T2 type transient of 6E-03/py.

Reducing the Oconee T2 core-melt frequency by the assumed initiating frequency of 6.0E-04/py for overfeed gives a predicted core-melt frequency due to the transient nature of the scenario of (3.44E-05/py)(6.0E-03/3) = 6.88E-08/py.

Total Core-Melt from SG Overfill with MSLB, and Transient Shutdown

The total estimated core-melt frequency due to transient shutdown from turbine damage or MSLB is then estimated to be (6.27E-08 + 6.88E-08)/py = 1.32E-07/py.

Public Risk for SG Overfill with MSLB, and Transient Shutdown

The public risk associated with the transient sequences for the Oconee plant is primarily associated with PWR release categories 3, 5, and 7 as shown in Table 2.1. This distribution will be used here for both transient and MSLB scenarios. Again, equating core damage from MSLB and core-melt is considered conservative.

TABLE 2.1. Public Risk Associated with Steam Generator Overfill with MSLB, and Transient Shutdown

Release Category	Probability	Man-rem/release	Frequency/py	Man-rem/py
PWR-3	0.5	5.4E+06	1.32E-07	3.56E-01
PWR-5	0.0073	1.0E+06	1.32E-07	9.64E-04
PWR-7	0.5	2.3E+03	1.32E-07	1.52E-04
Total				3.57E-01

The estimate of public risk is then 3.57E-01 man-rem/py. The conservative assumptions are the high operator failure rate, and certain failure of the PLS given spillover.

2.3 PROGRESSION OF SCENARIO TO SGTR AND CORE-MELT

Given steam line failure, the accident will most likely progress as a simple cooldown transient. However, there is the potential for steam generator tube rupture due to the differential pressures generated in the blow-down. The probability of SGTR given steam line break has been addressed by the NRC

(NUREG-0844, NRC 1983a) as part of its evaluation of Unresolved Safety Issues A-3, A-4, and A-5. Based on observed experience, this probability is p (tube rupture following a MSLB) = 0.034. This was broken down as follows:

P (1 SGTR following MSLB) = 0.017

p (2 to 10 SGTRs following a MSLB) = 0.014

p (more than 10 SGTRs following a MSLB) = 0.003.

The report did differentiate by reactor type in considering plant response to the SGTRS. However, the probabilities of tube rupture were applied to all reactor types. As a result, it will be assumed here that these probabilities are applicable to the B&W Oconee plant. The initial plant response to tube ruptures can be modeled as a small break LOCA. However, the long-term system response to a SGTR may differ from that of a LOCA in that water released from the break may not be available for collection at sumps within the reactor building. Long-term recirculation modes may not be available as they would be for most LOCAs.

To model the plant response to a SGTR, PNL examined the specific event tree developed for this purpose for the Oconee B&W PWR (NSAC-60, EPRI 1984) as well as information developed in support of unresolved safety issues A-3, A-4, and A-5 concerning steam generator tube integrity (NUREG-0844). The results are summarized in Table 2.2 below.

TABLE 2.2. Core-Melt Contribution of SGTR Events for the Oconee PRA

Sequence	Core-Melt Type	Estimated Frequency, 1/py
R U	A	3.9E-07
R U	B	8.5E-07
R X O	A	4.0E-07
R X O	B	7.4E-07
Total		2.38E-06

In this table, the following definitions apply:

R = frequency of the SGTR event (greater than 100 gpm) = 8.6E-03/py
U = failure of high pressure injection (HPI)
X = failure to achieve long-term cooling at cold shutdown
A = core-melt with sprays available to scrub radionuclides
B = core-melt with sprays failed.

With the total predicted dominant contribution to core-melt from SGTR of 2.38E-06/py and a SGTR initiating frequency of 8.0E-03/py, the conditional probability of core-melt given SGTR is then 2.77E-04. This compares to the Zion Westinghouse PWR, where the conditional probability of core-melt given SGTR was 9.19E-06, or approximately 1E-05 given SGTR.

As pointed out in the PNL A-47 examination of MSLB leading to SGTR for the Westinghouse plant, the sequences developed in the PRAs do consider the potential for the HPI system to fail to successfully depressurize and cool the RCS following a SGTR. This centers on the early failure of the HPI itself, or exhaustion of the water inventory in the reactor water storage tank (RWST) before depressurization. The latter is highly dependent on the ability to isolate the affected steam generator.

In the PRAs, many scenarios for single and especially multiple tube rupture events postulate the lifting and sticking open of steam generator relief valves due to the large pressure spike seen by the secondary side when rupture occurs. However, this accident sequence is driven by an assumed steam line break on the secondary side, thus making the lift of relief valves unlikely. Failure to isolate the SG due to steam line rupture inboard of a main steam isolation valve (MSIV) is considered a potential contributor to tube rupture. However, this initiating frequency is quite low due to the low random potential for valve or steam line rupture. This then results in a small contribution to the total core-melt frequency for MSLBs inboard of the MSIV predicted in NUREG-0844.

In a spillover scenario, however, the potential for a steam line break inboard of the MSIVs may have a higher potential. The analysis here assumes that a steam line break occurs with high probability given overfill. If a conservative approach is further taken to assume a 50 percent probability of MSLB above or below the MSIV, then this scenario may play a dominant role in the resulting conditional probability of progression to core-melt. Note again that the Oconee plant has no MSIVs, but valves are present in the general population of B&W PWRs.

To determine the potential impact of the MSLB location on core-melt frequency, the appropriate scenarios and failure probabilities from NUREG-0844 Chapter 3.4 (NRC 1983a) were examined, with the results given below. They have also been coupled with the assumed SGTR probabilities. This same approach was used to model the Westinghouse plant response to MSLB and SGTR. Given the level of uncertainty in exact plant response, this is considered appropriate at this time.

Case 1: Rupture of Main Steam Line Inboard of the MSIV

Number of SGTRs	Probability of Rupture	Probability of Loss of RWST before RCS Depressurization	Probability of Failure to Isolate SG	Net Core-Melt Probability
1	0.017	1E-03	1	1.7E-05
2 to 10	0.014	1E-02	1	1.4E-04
more than 10	0.003	0.5	1	1.5E-03
Total Probability of Core-Melt Given MSLB Inboard of MSIV				1.66E-03
Conditional Probability of Core-Melt Given MSLB and SGTR				4.87E-02

Case 2: Rupture of Main Steam Line Downstream of the MSIV

Number of SGTRs	Probability of Rupture	Probability of Loss of RWST before RCS Depressurization	Probability of Failure to Isolate SG	Net Core-Melt Probability
1	0.017	1E-04	1E-03	1.7E-09
2 to 10	0.014	1E-03	1E-03	1.4E-08
more than 10	0.003	1E-03	1E-03	3.0E-09
Total Probability of Core-Melt Given MSLB Downstream of MSIV				1.87E-08
Net Probability of Core-Melt Given MSLB and SGTR				5.50E-07

For plants with MSIVs, a 50 percent probability of MSLB inboard of the MSIVs is used. The conditional probability of core-melt given MSLB and SGTR can then be weighted, giving (0.5)(4.87E-02 + 5.50E-07) = 2.44E-02. In B&W plants with MSIVs, the core-melt frequency would then be estimated to be lower by a factor of 2.

The Oconee plant is design specific in that no motor-operated MSIVs are present, only manual valves. As such, any failure in the steam line would likely result in loss of water collection in sumps for recirculation. This will thus be used at Oconee as well until better information is available as to the probable frequency and location of MSLB given spillover, giving a conditional probability of core-melt given SGTR of 4.87E-02.

In this analysis, the frequency of overfill progressing to spillover, MSLB and SGTR is (5.70E-03/py)(0.034) = 1.94E-04/py. Using this new initiating frequency for SGTR, the total predicted frequency of core-melt due to this control system failure is then (1.94E-04/py)(4.87E-02) = 9.45E-06/py.

Comparison to SBLOCA Response

PNL also examined the possibility of modeling the SGTR event with small break LOCA (SBLOCA) event trees from the Oconee PRA. With an initiating frequency of 1.3E-03/py for S3 (less than 4 inch) SBLOCAs, the resulting Oconee core-melt frequency due to S3 sequences was 1.56E-05/py, giving a conditional probability of core-melt given SGTR of (1.56E-05/py)/(1.3E-03/py) = 1.20E-02.

The approach used above increases the estimated frequency of core-melt by a factor of four compared to an analysis based on system response to a SBLOCA.

Pressurized Thermal Shock

The potential for MSLB or SGTR leading to pressurized thermal shock (PTS) and possible vessel rupture has not been fully evaluated at this time. The consideration of such events in the Westinghouse PWR has put preliminary estimates of vessel failure probability below 1E-06 given the PTS event, indicating that PTS would not contribute significantly to risk for events initiated by the control failures examined. The role of PTS should be examined specifically for the B&W plant design when the PTS program makes its conclusions.

2.4 PUBLIC RISK DUE TO STEAM GENERATOR OVERFILL AND SGTR

The core-melt sequences above were brought about by SGTR and subsequent exhaustion of the water storage tank inventory, and water not being available from the building sumps. As a result, the containment sprays would also be assumed to be inoperable. In addition, the release is characterized by a significant leakage of containment, given the SGTR and MSLB. Given these considerations, only release category 2 at 4.8E+06 man-rem/core-melt will be used to estimate the public risk, as was done with the PNL analysis of the Westinghouse PWR. The results are summarized in Table 2.3.

TABLE 2.3. Public Risk Associated with Steam Generator Overfill, MSLB, and SGTR

	A-47 PNL Analysis of Overfill with SGTR		
Release Category	Induced SGTR Core-melt/py	Core-melt/py Best Estimate	Man-rem/py Best Estimate
2	2.38E-06	9.45E-06	4.54E+01

2.5 RESULTS OF STEAM GENERATOR OVERFILL

The results of the consideration of steam generator overfill leading to a transient shutdown, MSLB, or progressing beyond MSLB to a SGTR are summarized

in the following table. Note that the simple consideration of the overfill as a transient requiring plant shutdown represents the major part of the risk estimated here. Again, these frequencies assume an overfill initiating frequency of 0.006/py considering both steam generators including a 0.7 failure probability of the operator to terminate the overfill. The probability of inducing a MSLB was then valued at 0.95, and probability of progressing to core damage given MSLB at 1.1E-05. Note also that the predicted core-melt frequency for MSLB is similar to that predicted for transient shutdown; however, the MSLB frequency actually predicts core damage and not core-melt.

The probability of SGTR given MSLB was then put at 0.034, and the resulting response modeled based on the assumption that the break occurs above an isolation valve in the steam line and outside the reactor building where water would not be collected by building sumps for recirculation.

Note that for Oconee the latter assumption is not particularly conservative as the plant is not equipped with operator-powered MSIVs. The plant may have manual valves on steam lines, but credit for their operation could not be assumed given a MSLB.

TABLE 2.4. Result of Overfill Scenario for Oconee

Sequence	Frequency	Core-Melt Frequency, 1/py	Public Risk, man-rem/py
		Best Estimate	Best Estimate
T2 Transient Shutdown	(0.006)	6.88E-08	1.86E-01
Overfill & MSLB	(0.006)(0.95)	6.27E-08	1.70E-01
		1.32E-07	3.56E-01
SGTR	(0.006)(0.95)(0.034) = 1.84E-04/py	9.45E-06	4.54E+01
TOTAL		9.58E-06	4.58E+01

3.0 ICS POWER FAILURES

The ORNL analysis of control system failures identified two Integrated Control System (ICS) related power failures that may lead to overfill and undercool events. These failures are analyzed further here.

3.1 LOSS OF ICS HAND POWER

The ORNL analysis identified an insufficient core cooling scenario involving the loss of ICS branch circuits HX or HX1. This is determined to result in the MFW pumps being run back to the minimum speed and the turbine bypass steam dump valves being closed. This then initiates a reactor and turbine trip on high RCS pressure.

The scenario as postulated by ORNL is that continuous MFW pump operation would block the initiation signal for Emergency Feedwater System (EFW) operation as no low MFW pump discharge pressure or trip signal would be generated. The steaming rate then exceeds feedwater input, and steam generator dryout will occur unless the operator manually initiates EFW within 30 minutes. Core-melt can also be prevented by initiating HPI within 60 minutes.

The frequency of this event is estimated by ORNL as follows:

- frequency of ICS hand circuit failure = 0.009/py
- probability of operator failure to initiate AFW within 30 min = 0.1
- probability of operator failure to initiate HPI within 60 min = 0.01.

The total sequence frequency is then put at (0.009/py)(0.1)(0.01) = 9E-06/py.

The power failure and trip cause closure of the turbine bypass and stop valve, seal the secondary side and maintain the steam pressure at a high enough level to prevent MFW flow. The ORNL simulation then predicts that pressures will cycle about the safety relief valve lift points, maintaining sufficient pressure in the secondary side to prevent MFW flow.

The question is then whether conditions can remain such that MFW flow is prevented for the 30-minute period after ICS hand power failure. With safety relief valves cycling several times during this interval the potential exists for a relief valve to stick open, thus depressurizing the secondary side. The Oconee PRA estimates this probability at 0.05 per demand. The probability of failure to depressurize to allow MFW flow then will be a function of the number of valve lifts experienced in the 30-minute period. For example, 5 lifts would reduce this probability to (0.95)**5 = 0.77. Ten lifts would reduce this to (0.95)**10 = 0.6. To be conservative, it will simply be assumed that relief valve sticking is possible, but no credit will be taken for this at this time. Successful cooling will then rely on operator action to initiate MFW or EFW flow during the 30-minute period.

The event tree for this scenario is shown in Figure 3.1. The potential for passive recovery of feedwater flow during the 30-minute period preceding dryout is included, reflecting the potential for relief valve depressurization of the secondary side. The probability of this failing is, however, placed at 1 at this time.

The ORNL estimate for operator failure to reestablish MFW or EFW flow is put at 0.1 and failure to initiate HPI at 0.01. These values are consistent with the estimates used for operator performance in the Oconee PRA sponsored by the NRC (Kolb et al. 1981). Note that failure of the H1X power circuit will be annunciated directly in the control room (alarm A1-24, control board UBI, NSAC/60, page A9-31). The probability of operator detection and correction could thus be higher than assumed here.

The net result is an estimated core-melt frequency of 9.0E-06/py.

3.2 PUBLIC RISK DUE TO LOSS OF ICS HAND POWER

This scenario then progresses to core-melt given the failure of feedwater or high pressure injection systems. In the Oconee PRA, core-melts as a result of such system failures are characterized by release categories 3, 5, and 7, with a probability distribution of 0.5, 0.0073, and 0.5, respectively. Using the associated man-rem/release factors as presented in the Value/Impact Handbook (Heaberlin et al. 1983), the resulting estimate of public risk represented by this scenario is shown in Table 3.1.

TABLE 3.1 Public Risk Associated With ICS Hand Power Failure

Core-Melt Frequency, 1/py	Release Category	Probability	Man-Rem Per Release	Man-Rem Per Plant-Yr
9.0E-06	3	0.5	5.4E+06	2.43E+01
	5	0.0073	1.0E+06	6.57E-02
	7	0.5	2.3E+03	1.04E-02
				2.44E+01

The total public risk is then estimated at 2.44E+01 man-rem/py. ORNL made no estimate of the upper bound for the initiating frequency. The upper bound will simply be assumed here to be a factor of 10, giving an upper bound on core-melt of 9E-05/py, and an upper bound on risk of 2.44E+02 man-rem/py.

3.3 LOSS OF ICS AUTO POWER

The ORNL analysis also evaluates the loss of ICS auto power on the H or H1 branches.

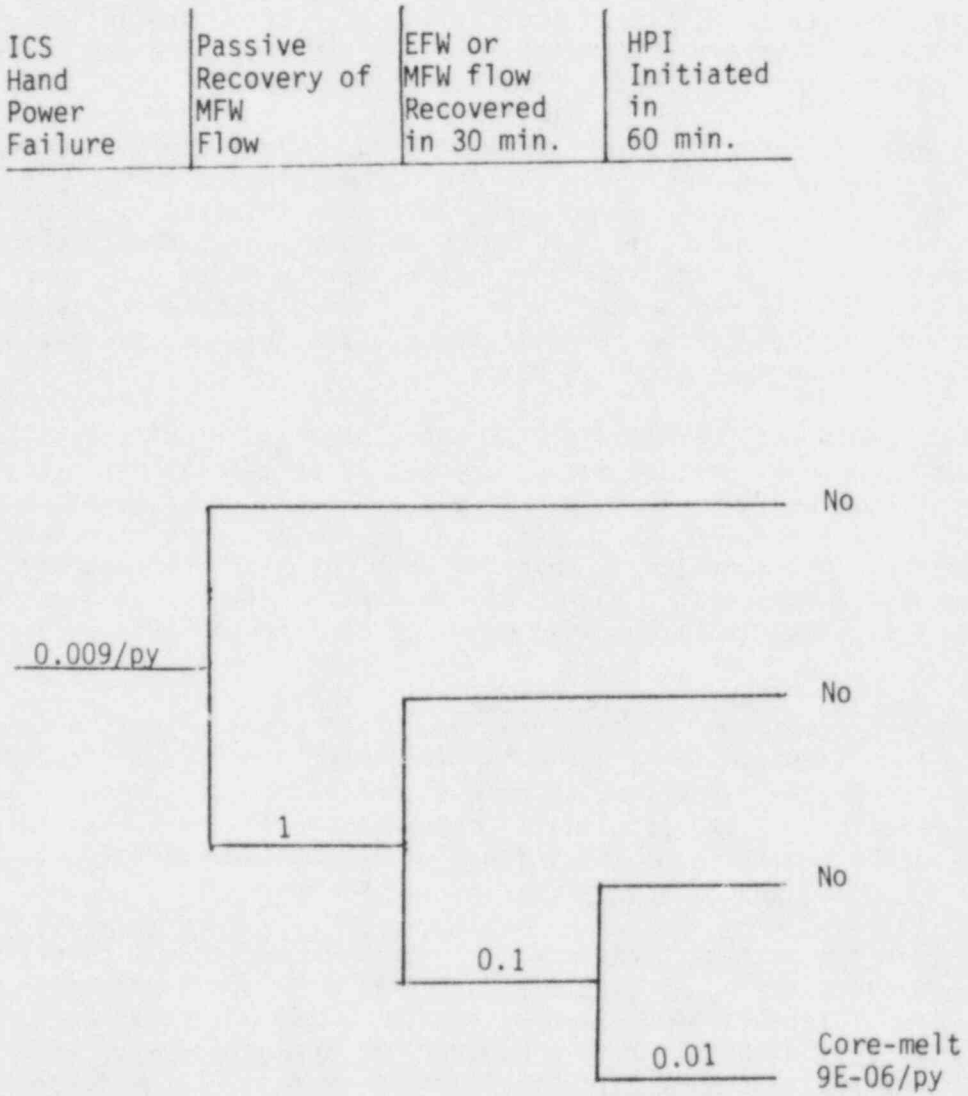

FIGURE 3.1 Loss of ICS Hand Power Event Tree

The ORNL core-melt event tree associated with the loss of ICS auto power, assuming that Oconee MFW pumps do not trip automatically, is given in Figure 3.2. As can be seen, the primary contribution to failure comes from operator failure to isolate the MFW pumps, and then failing to initiate EFW or HPI 30 to 60 minutes after MFW isolation when the scenario becomes an undercooling event.

The ORNL study indicates, however, that operation could continue with failure of the ICS auto power as the system is in an unstable equilibrium with respect to feedwater flow. Instrument drifts, etc., would then be expected to eventually cause an out-of-balance condition generating a trip signal. ORNL puts this probability at 1, and assigns operator error probabilities on the assumption that they are responding to a reactor trip after an instability occurs, without any prior indications as to the cause.

PNL has concluded that the operator response will be highly dependent on the recognition of the ICS power failure. Once alerted to the power failure, the probability of successful operator action in maintaining stability of the plant before a trip occurs is thought to be much higher than reflected in the ORNL numbers. The operator can continue operation in manual control or induce plant shutdown. The probability of failure to maintain adequate feedwater flow under manual control during operator-induced shutdown would likewise be expected to be smaller than that given by ORNL.

ORNL points out that loss of ICS auto power would not result directly in a transient. However, the automatic response to perturbations in the plant operating state would be limited. It was assumed that an eventual plant trip would occur in response to such perturbations (e.g., a main feedwater control valve drift). The question is then how long the plant can operate in this unstable equilibrium state, and whether operator detection and correction of plant condition is likely compared with operator response to an off-normal plant trip.

An event tree based on continued operation after detection of the auto power failure is shown in Figure 3.3. The event tree is developed for a 0.9 probability of detection, resulting in a significant reduction in the core-melt frequency estimate. The probability of operator failure to maintain feedwater controls after detection of the failure would be lower compared to responding to a trip.

The event tree then centers on a reasonable estimate of operator detection of the ICS circuit H or H1 power failure before an upset condition develops. An ORNL review of the Oconee plant indicates that the H circuit failure would be annunciated in the control room. However, no annunciators or alarms were found directly related to the H1 circuit, which feeds most of the feedwater control circuits. Oconee personnel indicated that they would respond to the failure by taking manual control and maintaining reactor operation as depicted in Figure 3.3; however, no existing procedures were found for such a failure.

As a result, the more conservative Figure 3.2 as developed by ORNL will be used at this time. It should be recognized, however, that proper annunciation and operator response could reduce the scenario frequency significantly.

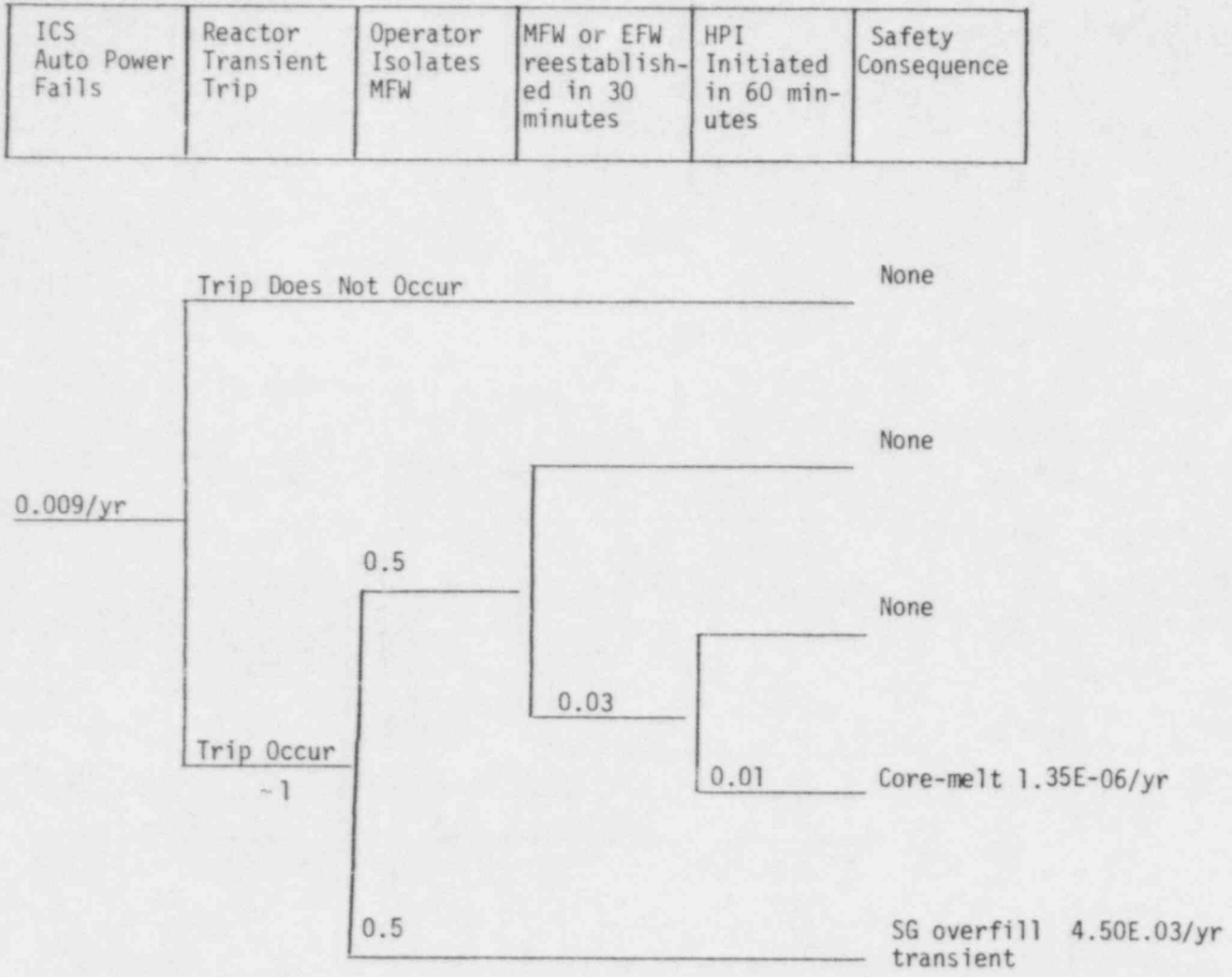

FIGURE 3.2. SAI ICS Auto Power Failure Event Tree

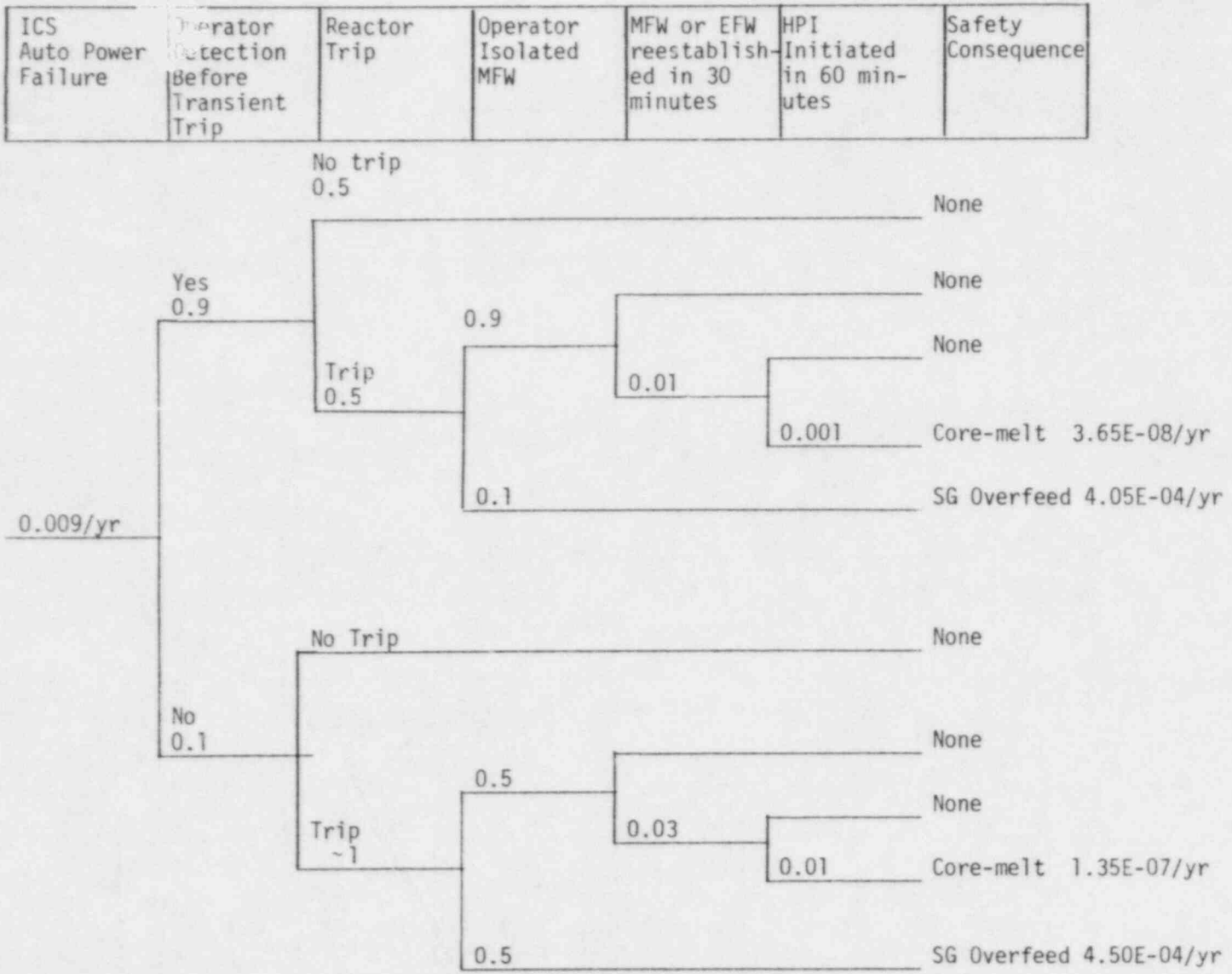

FIGURE 3.3. Proposed PNL Modification of ICS Auto Power Failure Event Tree

Core-Melt Frequency

The frequency of this scenario progressing to core-melt is 1.35E-06 in Figure 3.2, with another branch progressing to overfill with a frequency of 4.50E-03/py. Note, however, that given the auto power failure, the high level MFW pump trips still are functional. As a result, the MFW pumps will trip if the operator fails to isolate them. From an operational standpoint, the demands placed on the plant certainly favor the operator action in throttling feedwater flow. However, in this development of risk, there is no real distinction between operator and automatic MFW isolation. Both will eventually require operator re-initiation of flow within 30 minutes to prevent dryout. Note also that the latest ORNL simulations indicate that the feedwater pumps may trip themselves on runout after reactor trip, making Figure 3.2 applicable. As a result, the last branch will also contribute to core-melt with a frequency of 1.35E-06/py, for a total estimated frequency of 2.70E-06/py. Again, it will be assumed that the upper bound is a factor of 10 higher or 2.70E-05/py.

Progression of Overfill to Spillover and MSLB

To present a potential for MSLB, PNL has assumed that the overfill must progress to the point of actual spillover into the steam lines. The overfeed as analyzed by ORNL is expected to result in MFW pump trip due to low suction pressure, or, if this does not occur, all MFW pumps trip on high level in either SG. Either trip would end the overfeed. To be conservative it will be assumed that trip on low suction does not occur, with release on the high level trip. In this case, that would require the failure of the high level trip on demand. The ORNL estimate of an undetected failure existing giving a failure probability on demand of 0.047 will be used here, giving a spillover frequency of (4.50E-03/py)(0.047) = 2.12E-04/py.

The potential for MSLB given overfill has then been estimated by PNL to be 0.5 given that spillover occurs after plant trip. This is reduced from 1.0 for spillover during operation, assuming that the conditions that might drive a possible pipe failure are reduced. The frequency of MSLB is then put at 1.06E-04/py due to this scenario. The probability of further progressing to core damage given MSLB was put earlier at 1.1E-05, giving a final estimate of the frequency of core damage following overfill and MSLB at 1.16E-09/py. The upper bound is again a factor of 10 higher, or 1.16E-08/py.

Progression to Spillover and T2 Transient Shutdown

As with the first spillover scenario, this scenario has the potential for damaging the PCS necessary for successful shutdown and decay heat removal. The overfill and progression to spillover could then be considered a transient initiator even if no MSLB occurs. Again using the 0.5 operator error probability for MFW control and 0.047 for failure of the high trip, and a 0.1 factor for failure of the PCS, the T2 initiating frequency for this sequence becomes (0.009/py)(0.5)(0.047)(0.1) = 2.12E-05/py. Ratioing this to the Oconee T2 frequency of 3/py gives the predicted core-melt estimate of (2.12E-05/3)(3.44E-05/py) = 2.43E-10/py. This contribution is negligible for all practical purposes.

Progression of Overfill to Spillover, MSLB, and SGTR

The probability of SGTR given MSLB was estimated earlier at 0.034. The probability of core-melt given MSLB and subsequent SGTR was also put at 2.44E-02. The net result is an estimated probability of core-melt given overfill, spillover, MSLB, and SGTR of (4.5E-03/py)(0.047)(0.5)(0.034)(2.44E-02) = 8.77E-08/py. The upper bound is again assumed to be a factor of 10 higher.

The total estimated core-melt frequency is then (2.70E-06 + 1.16E-09 + 8.77E-08)/py = 2.79E-06/py, with an upper bound a factor of 10 higher.

3.4 PUBLIC RISK DUE TO LOSS OF ICS AUTO POWER

The release categories associated with a failure of feedwater, HPI, or core damage due to MSLB were assumed earlier to be release categories 3, 5, and 7, with the probability distribution of 0.5, 0.0073, and 0.5, respectively. The SGTR scenario is assumed to be associated entirely with release category 2. The results are shown in Table 3.2.

TABLE 3.2. Public Risk Associated with Failure of ICS Auto Power

Core-Melt Frequency, 1/py	Release Category	Probability	Man-Rem Per Release	Man-Rem Per Plant-Yr
Case 1: Overfill with Operator Failure to Initiate Feedwater or HPI				
2.70E-06	3	0.5	5.4E+06	7.29E+0
	5	0.0073	1.0E+06	1.97E-02
	7	0.5	2.3E+03	3.11E-03
				7.31E+0
Case 2: Overfill with Subsequent MFW High Trip Failure, and MSLB				
1.16E-09	3	0.5	5.4E+06	3.13E-03
	5	0.0073	1.0E+06	8.47E-06
	7	0.5	2.3E+03	1.33E-06
				3.14E-03
Case 3: Overfill with Subsequent MFW High Trip Failure, MSLB and SGTR				
8.77E-08/py	2	1.00	4.8E+06	4.21E-01

The total public risk is then estimated at (7.31E+0 + 3.14E-03 + 4.21E-01) = 7.73E+0 man-rem/py. No estimate of the upper bound for the initiating frequency was made by ORNL. This will simply be assumed here to be a factor of 10, giving an upper bound on core-melt of 2.79E-05/py, and an upper bound on risk of 7.73E+01 man-rem/py.

4.0 VALUE/IMPACT ANALYSIS

In this chapter, several modifications to the plant will be postulated to evaluate the potential cost and associated reduction in risk.

4.1 MODIFICATIONS TO REDUCE UNDETECTED FAILURE OF THE HIGH-LEVEL MFW TRIP

ORNL suggests that the potential for undetected failure could be reduced by modifying the high-level trip logic, or by reducing the time between inspection periods. These issues are discussed below.

The initial overfill scenario developed by ORNL centers on the failure of the high-level MFW trip function in an undetected state. The assumed component failures and equivalent failure on demand probabilities calculated by ORNL are given below, based on an annual inspection rate with 50 percent of the failures being detected and repaired in that period:

A) either MFW pump intercept valve fails	0.001/demand
B) either MFW pump trip solenoid valve fails	0.006/demand
C) MFW pump trip relay FTPX fails	0.009/demand
D) either SG operate range level transmitter fails	0.004/demand
E) either multiplication module fails	0.018/demand
F) either signal monitor module fails	0.007/demand
G) either signal generator module fails	0.002/demand
Total	0.047/demand

The problem centers on the current configuration of the high-level trip circuit. This consists of two parallel circuits acting on signals from generator A and B, respectively, each with two trip relays in series (i.e., one from each of two level transmitters in the generator), as shown in Figure 4.1. To produce the trip signal, both level transmitters in a generator must then send a high signal, and both associated normally-open relays in one parallel branch of the trip circuit must close. High signals from the other generator would act the same. This could be termed a 2-out-of-2-once trip logic, as a high-level condition in either generator could produce the trip. These parallel circuits then feed to one FTPX solenoid/contact which provides another single failure point as listed above.

ORNL suggests that the trip relays acting on signals from the two level transmitters in each generator could be wired in parallel rather than series, thus lowering the potential for one to fail in the open condition. The function of the FTPX relay would also have to be duplicated in parallel if this advantage is to propagate through the entire trip circuit. It was pointed out, however, that this would increase the potential for spurious trips.

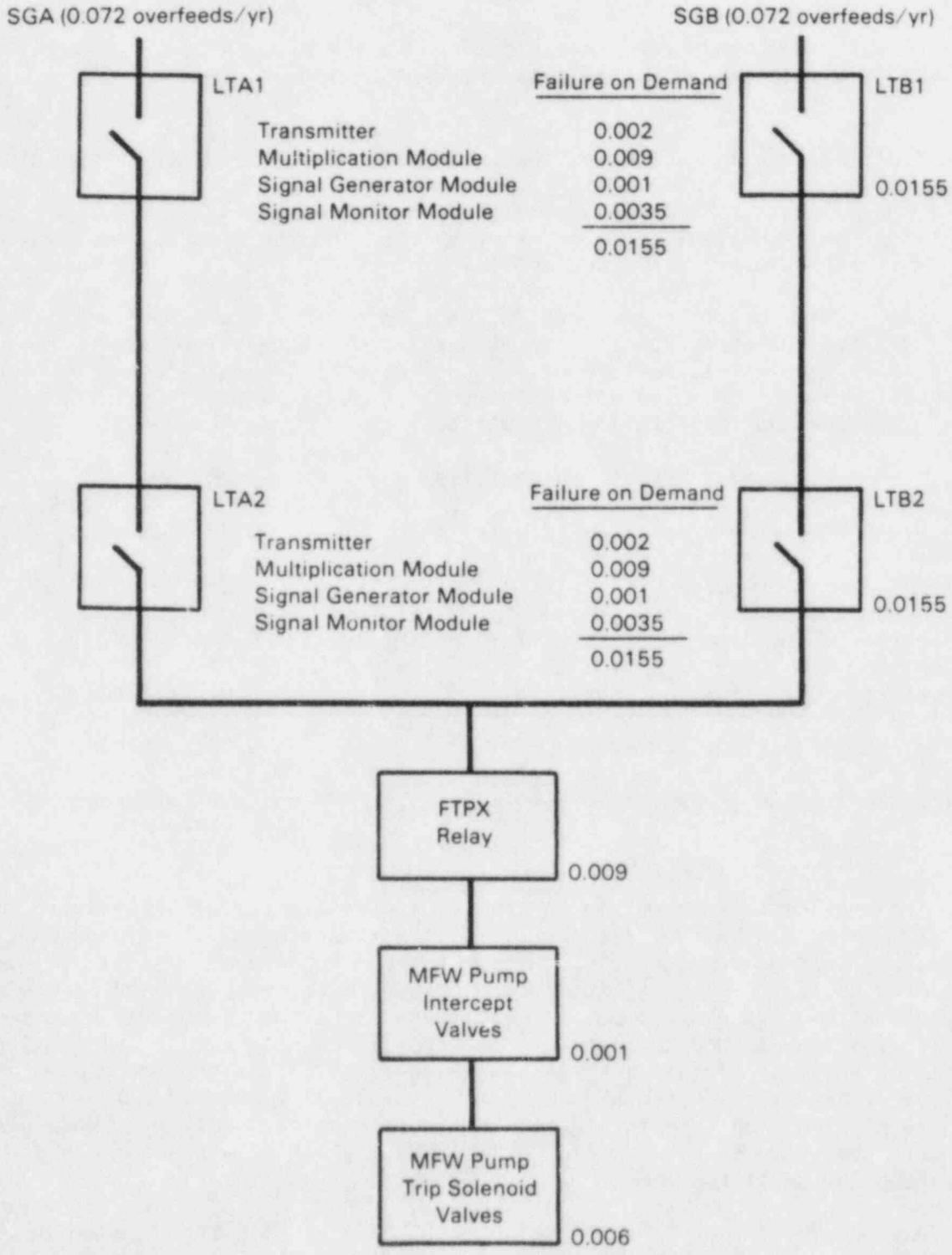

FIGURE 4.1. B&W Oconee PWR High Level MFW Trip Circuit

However, a simpler approach based on reducing the period between testing may provide as much or more benefit using the same basic circuit logic. Discussions with the ORNL subcontractor (McBride, Science Applications Inc.) indicated that the annual inspection and calibration period assumed is the major contributor to the undetected failed state. The probability of failure on demand could likely be reduced in direct proportion to the inspection period. As a result, monthly inspections or inspections on each shutdown could reduce the assumed failure probability by a factor of 10 across the board for all these failures listed above.

It is uncertain if such testing can be accomplished during plant operation on all components listed above, particularly the pump valves and trip solenoids themselves. However, level transmitter outputs can be checked in comparison to other outputs, and signal module outputs can be tested on generator A, then generator B. After consultation with ORNL, this is thought to reduce all factors above by a factor of two percent except a, b, and c, giving an estimated reduction in the high trip failure of (0.50)(0.047 - 0.016)/(0.047) = 0.33. This would reduce the core-melt frequency proportionally, giving a reduction of (0.33)(9.58E-06/py) = 3.16E-06/py. The public risk would also be reduced by (0.33)(4.58E+01 man-rem/py) = 1.51E+01 man-rem/py or 4.53E+02 man-rem/plant over 30 years.

The development of new testing procedures is estimated to require two people for two months, or 16 man-weeks at $2270/man-week using the costs suggested in NUREG/CR-3568 (Heaberlin et al. 1983). This gives a development cost of $36,320.

The current effort required annually to inspect these circuits is not known. As a conservative estimate, it will be assumed here that this requires one man-day per inspection, or currently (1/5) ($2270/py) = $450/py. Increasing the inspection rate to once a month would then raise this to $5.5E+03/py. Assuming a 10 percent discount rate over 30 years, this represents a cost of (9.43)($5.5E+03) = $5.2E+04. The total cost is then $5.2E+04 + $36,320 = $8.8E+04 per plant.

The value/impact ratio is then estimated at 4.53E+02 man-rem/$8.8E+04 = 5.2 man-rem/$1000.

Addition of Parallel FTPX Relay With Monthly Testing of Trip Function

The circuit as it is currently installed has the two trip relays associated with steam generator A (SG A) level transmitters and the two from SG B feeding a signal to one FTPX relay. Simply adding an additional FTPX relay to the circuit such that the trip signal from SG A and SG B have their own associated FTPX relay does not change the logic arrangement or theoretical failure probability compared to the original configuration. However, feeding the signals from either generator into two relays in parallel will give an assumed failure probability of (0.009)(0,009) = 8.1E-05/demand. In addition, the circuit can be wired to allow for testing of trip relays while still providing overfill protection for each generator. It will be assumed here that an additional FTPX relay is wired to allow for such testing, with modifications to all components except the valves themselves to allow online testing.

This is thought to reduce all factors mentioned above by 90 percent except A and B, giving a estimated reduction in the high trip failure of (0.90)(0.047 - 0.007)/(0.047) = 0.766. This would reduce the core-melt frequency proportionally, giving a reduction of (0.766)(9.58E-06/py) = 7.34E-06/py. The public risk would also be reduced by (0.766)(4.58E+01 man-rem/py) = 3.51E+01 man-rem/py or 1.05E+03 man-rem/plant over 30 years.

The cost of adding the additional relay is estimated here as follows:

- two man-weeks of engineering support
- one man-week of craft services for installation
- $5,000 in equipment cost.

This gives a total of $11,810, or approximately $12,000 in addition to the $8.8E+04. This will be assumed to double for additional changes in wiring to allow full operational testing of the other components in the circuit. This gives a total of $1.88E+05, or approximately $2E+05.

This gives a value/impact ratio of 1.0E+03 man-rem/$2E+05 = 5.3 man-rem/$1000. The ratio is thus improved slightly with the addition of the parallel FTPX relay and full operational monthly testing compared to monthly testing only.

Modifications to Close Feedwater Block Valves

The Oconee plant uses separate feedwater delivery lines for the main and auxiliary feedwater systems. The potential then exists for use of the block or isolation valves on the feedwater lines to terminate the overfill. Referring back to Figure 4.1, it can be seen that if the same level transmitters are used for a signal to the block valves, the maximum increase in reliability will be represented by removing the failure contribution from the solenoid and intercept valves on the steam lines to the MFW turbines. This represents a possible reduction of (0.007/0.047)(4.58E+01 man-rem/py)(30 yrs) = 205 man-rem. The modification is thus not very effective, eliminating only approximately 15 percent of the risk with a bounding cost of $205,000 to stay under the 1 man-rem/$1,000 criterion.

Note, however, that if an independent level transmitter signal is used, the estimated failure probability of an independent trip to the block valve would be put at (0.0155 + 0.009 + 0.001) = 0.0255 for a transmitter, FTPX relay, and block valve. The failure on demand of the entire trip circuit would then be (0.047)(0.0255) = 1.2E-03/demand, for a reduction of (1 - 1.2E-03/0.047) = 0.974.

The risk reduction would then be (0.974)(4.58E+01 man-rem/py)(30 yrs) = 1.34E+03 man-rem over 30 years. The addition of a new trip circuit using a block valve would then be very effective in reducing the frequency of overfills, with costs up to $1.34E+06 acceptable for a value/impact ratio of 1 man-rem/$1,000 or better.

The indications are that the startup range level transmitters would be of possible use for this new trip function. If so, expenditures for this modification would be limited to the wiring and relays required. This is estimated here as follows:

- 2 man-weeks of engineering support at $2270/week
- 8 man-weeks of craft services
- $20,000 in hardware and supplies
- $20,000 for a safety evaluation of the trip circuit.

This totals $82,700 for a value/impact ratio of 1.34E+03 man-rem/$82,700 = 16.2 man-rem/$1,000. Note that costs would have to exceed approximately $250,000 to get a value/impact ratio on the order of or smaller than that estimated for modifications to allow monthly testing of the existing trip circuit (i.e., 5.3 man-rem/$1,000) as estimated previously.

Modifications to Trip Logic

In the PNL examination of the GE BWR and Westinghouse PWR, the installation of a 2-out-of-4 trip logic was examined but did not appear to be favorable. In the Oconee B&W PWR plant, the output from the level transmitters is not being used as a level control signal to maintain an exact steam generator water level as in the previously mentioned plants. Rather, the B&W design operates with the water level falling within a broad operating range. Conditions are maintained within this range to give the proper degree of steam superheat at the generator output rather than to maintain a set water height. The operation of the ICS control loop is developed in detail in the ORNL report.

Because the GE and Westinghouse designs combine the feedwater level control and trip functions with the level transmitters, a failure there that could both fail the high trip and drive the feedwater increase becomes the dominant failure mechanism. Fixes addressing the level transmitter failure modes and logic then became the obvious targets for correction. With the separation of these functions in the B&W design, the dominant failure identified by ORNL became an undetected failure of the high trip. As such, corrective actions should be directed at this failure specifically for the B&W plant.

In the B&W plant, the ICS system relies on control of the feedwater valves as the first level of defense in preventing overfill of the steam generators. This in itself provides a high level protection function. The MFW pump trip function then operates independently of the ICS control loop. As such, the system already provides backup protection from overfill progressing to spillover. The question is what is the best way to improve this reliability.

Going to a multiple high-level trip logic system may theoretically improve the reliability of the trip, but on a practical level most of the benefits associated with a 2-out-of-3 or 2-out-of-4 trip logic are derived by allowing the ability to test the function during operation. Because the trip function is not used directly in control of the B&W design, the minor modifications postulated above essentially provide this ability without installing these more complicated logic networks. Putting the existing network of trip relays in parallel for a 1-out-of-1 logic would be less costly; however, the potential then exists for an increased rate of spurious trips, as pointed out by ORNL.

However, several modifications to the trip logic will be examined here for comparison. These are listed below in Table 4.1. The failure probabilities used for relays and modules are based on the values from ORNL. Note that the current circuit has two level transmitters and associated modules (multiplication, signal monitor, and signal generator modules) in series for a total failure probability of (0.004 + 0.018 + 0.007 + 0.002) = 0.031. It is assumed here then that one level transmitter and associated modules have a failure probability of 0.5(0.031) = 0.0155. This logic is shown more clearly in Figure 4.1. This again is the probability for failure on demand calculated by ORNL based primarily on undetected failures over the annual inspection period.

Note also that it will be assumed that the failure probability of the MFW valves themselves will bound the possible reductions here for the trip circuit. This is put at (0.001 + 0.006) = 0.007 out of the total of 0.047. This is 0.007/0.047 = 14.9 percent of the total failure probability, implying that a perfect trip logic providing a trip signal to the valves could only reduce the failure probability by 85.1 percent. This "perfect" logic would then correspond to a risk reduction of 0.851(4.58E+01 man-rem/py) = 3.90E+01 man-rem/py or 1.17E+03 man-rem over 30 years.

TABLE 4.1. Alternate Configurations for the B&W Oconee PWR High Level MFW Trip Function (Annual Testing Assumed)

Case	Configuration	Failure on Demand	Ratio of Alternate to Base Case, n	1-n
1	Base Case, 2-out-of-2, (total of 4 LTs and 1 FTPX)			
	2 LTs in series per SG	0.0155 + 0.0155		
	1 FTPX relay in series	0.009		
	MFW valves	0.007		
		0.047	1.0	0
2	2-out-of-2, extra FTPX (total of 4 LTs and 2 FTPX , annual testing)			
	2 LTs in series per SG	0.0155 + 0.0155		
	1 FTPX relay per SG	0.009		
	MFW valves	0.007		
		0.047	1.0	0
3	1-out-of-1, (total of 2 LTs and 1 FTPX)			
	1 LT per SG	0.0155		
	1 FTPX	0.009		
	MFW valves	0.007		
		0.0315	6.70E-01	0.33
4	1-out-of-2, 1 FTPX (total 4 LTs and 1 FTPX)			
	2 LTs in Parallel per SG	0.0155**2		
	1 FTPX	0.009		
	MFW valves	0.007		
		1.62E-02	3.46E-01	0.654

TABLE 4.1 (Continued)

Case	Configuration	Failure on Demand	Ratio of Alternate to Base Case, n	1-n
5	2-out-of-3, 1 FTPX (total 6 LTs and 1 FTPX)			
	3 LTs in Parallel per SG	3(0.0155)**2 +0.0155**3		
	1 FTPX relay	0.009		
	MFW valves	0.007		
		1.67E-02	3.55E-01	0.645
6	1-out-of-2, 2 FTPX (total 4 LTs and 2 FTPX)			
	2 LTs in Parallel per SG	(0.0155)**2		
	with FTPX relays in	(0.009)**2		
	in parallel MFW valves	0.007		
		7.32E-03	1.56E-01	0.844
7	2-out-of-3, 2 FTPX (total 6 LTs and 2 FTPX)			
	3 LTs in Parallel per SG	3(0.0155)**2 + (0.0155)**3		
	with 2 FTPX relays	(0.009)**2		
	in parallel MFW valves	0.007		
		7.81E-03	1.66E-01	0.834
8	2-out-of-4, 1 FTPX (total 8 LTs and 1 FTPX)			
	4 LTs in Parallel per SG	4(0.0155)**3 + (0.0155)**4		
	1 FTPX relay	0.009		
	MFW valves	0.007		
		1.60E-02	3.40E-01	0.66
9	2-out-of-4, 2 FTPX (total 8 LTs and 2 FTPX)			
	4 LTs in Parallel per SG	4(0.0155)**3 + (0.0155)**4		
	2 FTPX relays	(0.009)**2		
	in parallel MFW valves	0.007		
		7.10E-03	1.51E-01	0.850
10	No MFW Trip	1/0.047 = 21 (i.e. without other modifications, removal of the high trip would increase risk by a factor of 21 over the current base case).		

LT = level transmitter

Note that as in the PNL examination of alternate high level trip configurations for the GE and Westinghouse plants, the 1-out-of-1 configuration appears to be theoretically preferable to the 2-out-of-2 configuration. This is because the latter is subject to 2 single transmitter failures that could defeat the function versus 1 for the 1-out-of-1 configuration. More realistic evaluations must, however, consider the potential for spurious trip signals as well. Using the mean of 0.17 feedwater increases per year in 1 loop reported to date for B&W plants as a likely measure of level failures (EPRI 1982), one transmitter could result in 0.17/yr(30 yrs) = 5 spurious trips over a plant lifetime. Requiring 2 independent failures would reduce this to (0.17)(0.17)(30), or approximately 1 spurious trip. The true cost penalty for the simpler trip logics can then be significant over the lifetime of the plant. This will be considered further below.

Costs of Proposed Modification

The cost estimated earlier of $12,000 for one additional FTPX relay will be used here to estimate costs for additional relays or modules.

The cost of adding a level transmitter and associated relays to an existing 2-inch instrument line was estimated in the PNL examination of Westinghouse PWRs and GE BWRs to be approximately $150,000 with costs approaching $1,000,000 if additional penetrations were to be required. The $150,000 per transmitter figure will be used here.

The cost of removing LTs for less complicated systems is estimated at $12,000 per LT. For Case 3 below with a 1-out-of-1 trip on each generator, the cost would then be put at $24,000.

For Case 4 no hardware is added, and only the trip logic is modified to a 1-out-of-2 instead of a 2-out-of-2. The cost here is estimated as similar to adding a relay, or $12,000.

These figures were then multiplied by the number of transmitters or relays added to give the desired modification in Table 4.1, with the resulting risk reduction, cost, and value/impact given in Table 4.2. The configurations given are per generator, i.e., a 2-out-of-2 level transmitter configuration implies that each generator has 2 transmitters, for a total of 4.

The cost of a spurious trip is put at 24 hours of downtime, at $300,000 per day for replacement power costs (Andrews et al. 1983). The simpler configurations will be more subject to such trips; however the others may also suffer from several such trips over the lifetime of the plant. As a result the value/impact ratios are presented in Table 4.2 with 2 spurious trips considered for the 1-out-of-1 configurations, as well as without consideration of trips for comparison.

TABLE 4.2. Risk Reduction, Costs, and Value/Impacts of Alternate Configurations

Configuration	Risk Reduction Man-Rem Per py	Risk Reduction Man-rem 30 yrs	Cost $1000	Value/Impact Man-rem/$1000
1. 2-out-of-2, 1 FTPX with testing	1.5E+01	4.53E+02	88	5.2
2. 2-out-of-2, 2 FTPX with testing	3.51E+01	1.05E+03	200	5.3
3. 1-out-of-1, 1 FTPX with two spurious trips in 30 years	1.51E+01	4.53E+02	624	0.73

TABLE 4.2. (Continued)

Configuration	Risk Reduction Man-Rem Per py	Man-rem 30 yrs	Cost $1000	Value/Impact Man-rem/$1000
4. 1-out-of-2, 1 FTPX with two spurious trips in 30 years	3.00E+01	8.99E+02	612	1.47
5. 2-out-of-3, 1 FTPX	2.95E+01	8.86E+02	300	3.0
6. 1-out-of-2, 2 FTPX with two spurious trips in 30 years	3.87E+01	1.16E+03	624.00	1.86
7. 2-out-of-3, 2 FTPX	3.82E+01	1.15E+03	312	3.7
8. 2-out-of-4, 1 FTPX	3.02E+01	9.07E+02	600	1.5
9. 2-out-of-4, 2 FTPX	3.89E+01	1.17E+03	612	1.91

* Implementing equipment modifications as per calls 3 through 9 after monthly testing would reduce associated value/impact by approximately a factor of 10.

Note that hardware changes appear possibly favorable when considered alone. However, implementation after the simple monthly testing is applied would significantly reduce the estimated value of such hardware changes.

It must be noted that monthly instead of annual testing gives a similar risk reduction and value/impact ratio. This alone was postulated to act on 85 percent of the variables contributing to the trip failure (0.04/demand out of 0.047/demand, with 0.007 or 15 percent due to MFW valve failure), resulting in a 76.6 percent reduction in the sequence risk of 4.58E+01 man-rem/py. When the 15 percent contribution from the MFW valves is removed, the further modifications would be acting on only (100 - 76.6 - 15) = 8.5 percent of the risk, giving 3.89 man-rem/py or 1.17E+02 man-rem in 30 years. This essentially reduced the estimated value/impact ratio for hardware changes by a factor of 10. The NRC must then weigh these additional judgmental factors in deciding if the current system is inadequate, and to what level improvements will be required.

Limitations and Real-World Considerations

Further real-world limitations bring into question the implementation of hardware changes first. It must be pointed out that any comparison between

different level control and high-level trips is highly conditional on a number of factors, including basic hardware and reliability, as well as operator response to system failures. These factors can include plant-specific differences in and compensations for a number of areas, including:

- type of level control (three element, one element)
- power supplies
- backup or alternate level displays
- instrument line plumbing configuration
- controlling level display
- controlling level record
- annunciators and alarms
- operator training and procedures.
- maintenance, general age and state of equipment.

Systems which rely more heavily on the operator for detection and correction of failures may also have more emphasis on level display, operator training and procedures. However, many of the variables impacting performance of the high level trip in the B&W plant are not fully defined. As a result, the above conclusions must be taken as only a preliminary review of the potential impact of other feedwater control configurations on the A-47 issue.

Finally, the Peach Bottom final safety analysis report (FSAR) (page 7.2-20) notes that in a GE BWR, a 1-out-of-2 configuration is theoretically more reliable than a 1-out-of-2-twice, which in turn is theoretically more reliable than a 2-out-of-3 configuration. This agrees with the basic finding presented in Table 4.1 for possible failure combinations that can lead to an undetected high trip failure in the Oconee plant. Considerations based on available failure data may change this conclusion slightly in practice. However, the FSAR goes on to say that the differences are slight, and in a practical sense are negligible. It indicates that the primary reason to choose the more sophisticated configuration is that it allows for testing during operation.

The indications are then that real-world considerations could easily overshadow theoretical calculations. As pointed out in the PNL BWR report (Bickford and Tabatabai 1985a), this could include hydraulic shocks which occur at different rates in separate instrument lines making some failure combinations of sensors more likely, or common mode failures of instruments due to faulty maintenance. The data currently available on component failure rates are not specific enough as to failure cause (i.e., shocks, faulty maintenance, etc.) and failure mode (i.e., inoperable low scale, drift low, etc.) to support specific recommendations based on theoretical calculations.

When coupled with the above considerations, plus the role of the operator and possible negative impacts on operational reliability and the unique dynamic control features of the B&W design, it becomes apparent that the implementation of monthly testing should be considered first, with modifications to equipment held to those necessary to allow full online testing of all relays and components in the trip circuit. These recommendations should be regarded as preliminary, with the recognition that they should be subjected to detailed evaluation.

4.2 MODIFICATIONS TO REDUCE ICS HAND POWER DRYOUT SCENARIO

Discussions with ORNL and the SAI contractor indicate that several modifications are possible to avoid the dryout scenario caused by the hand power circuit failure and MFW runback to the minimum setpoint. These include the following:

- trip MFW pumps on loss of hand power
- reset minimum runback setpoint for MFW pumps
- modify MFW controls to reset to 50 percent position on 0 voltage signal
- allow initiation of EFW via low level signal
- reduce operator error.

MFW Trip on Loss of ICS Hand Power

The most basic modification is to simply trip the MFW pumps on failure of the ICS hand power circuit. The EFW function would then automatically be initiated, terminating the dryout scenario.

Reset Minimum Runback Setpoint for the MFW Pumps

The feedwater pump rpm at its minimum setpoint is insufficient to deliver water into the steam generator given closure of the turbine stop and bypass valve. The minimum setpoint could simply be increased to provide greater output flow. The high-level trip functions are still in place, preventing overfill to the point of spillover.

Modify the MFW Controls to Reset to the 50 percent Position on 0 Voltage Signal

The system as it is currently designed gives a zero voltage signal to the pump speed control unit on loss of the hand power supply. This equates to a minimum setpoint, resulting in the runback. However, many of the control circuits are designed to operate on a +10 to -10 voltage range, with 0 volts providing the middle or 50 percent range reading.

ORNL indicates that Oconee may be unique in its 0 voltage/minimum runback configuration. As such, other B&W plants would already use this modification. Note that this would most likely result in transforming the dryout scenario to an overfill, but again the high trips are still functioning, thus preventing progression to spillover. On trip of the MFW pumps, the EFW system would again come into operation.

Allow Initiation of the EFW System Via Low SG Level Indication

The EFW system is prevented from initiating in this scenario by continued operation of the MFW system, even though this is resulting in steam generator dryout. The level signals indicating a low steam generator water level would be used to control EFW given operation. However, the level transmitter signals are not used as an actuation signal for the EFW system.

Reduce Operator Error

The failure of the ICS hand power circuit is annunciated as such in the control room. Procedures also exist for the proper control of feedwater flow. As a result, reductions via this approach would be less effective than those above.

Potential Risk Reduction

Any of the modifications above could be postulated to reduce the frequency of the accident progressing to dryout and core-melt by an order of magnitude. The reduction in core-melt frequency is then estimated at 90 percent, or (0.90)(9.0E-06/py) = 8.10E-06/py. The reduction in risk is also estimated at (0.90)(2.44E+01 man-rem/py) = 2.20E+01 man-rem/py or 6.59E+02 man-rem over 30 years.

The examination of this system by ORNL indicates that two 1E "startup range" level signals per SG currently are used for EFW valve control and could be used to provide an initiation signal. This modification would include the addition of SG level bi-stables and modification of existing EFW start logic within existing 1E cabinets (assuming space is available within the cabinets).

Costs and Value/Impact

The cost of any one or a combination of modifications could thus approach $659,000 per plant (considered to be extremely unlikely) and still give a value/impact ratio of 1 man-rem/$1000. Because of the relatively simple nature of the fixes, the value impact ratio will simply be assumed here to be greater than 1 man-rem/$1000.

4.3 MODIFICATIONS TO REDUCE ICS AUTO POWER OVERFILL SCENARIO

Discussions with ORNL and the SAI contractor indicate that several modifications are possible to avoid the overfill scenario caused by the ICS auto power circuit failure. These include the following:

- insure annunciation of the Auto power circuit failure in the control room
- provide emergency procedures to the operator for auto power failure
- allow initiation of EFW via low level signal.

Note that the plant was originally thought to continue operation in an unstable equilibrium, eventually leading to some off-normal condition and plant trip. The most recent simulations indicate that a feedwater-induced trip is likely. In any event, the high-level feedwater trips are still in place. The dominant risk from this scenario was then found to be the potential for the accident progressing to a dryout scenario, where the operator fails to reestablish feedwater or HPI flow.

PNL did carry the scenario one step further by assuming failure of the high trip and spillover, but this risk was found to be an order of magnitude

lower than that due to the dryout scenario. Fixes discussed in Section 4.2 to prevent the high trip failure would reduce this even further. Thus, fixes for this dryout scenario should address the need to reduce operator error in reestablishing flow, or in providing an automatic initiation of flow.

Annunciation of Power Failure and Emergency Procedures

In the ORNL examination of Oconee for auto power failure, no annunciators or alarms were found associated with the H1 circuit that serves the majority of the feedwater controls. As a result, the assumption was made that no such indications are currently present. Discussions with Oconee operating personnel indicated that their response to an auto power failure would be to attempt stabilization of the plant through manual feedwater control, indicating that operator awareness of feedwater conditions would be high. However, no specific emergency procedures were found, and again reduced credit was taken for alert operator action in the risk calculation, which assumed an error probability of 0.03 for establishing feedwater flow in 30 minutes.

Assuming that annunciation of the failure and emergency procedures did exist, the operator error would be re-estimated at 0.01, the value used for failure to initiate HPI. The reduction in core-melt would then be 1.8E-06/py, and the reduction in risk would be (2/3)(7.73E+0 man-rem/py) = 5.15E+0 man-rem/py or 1.55E+02 man-rem over 30 years.

As a rough estimate, the cost for providing annunciation of the power failure is estimated to require the following:

- one man-month of engineering support
- two man-months of craft services for installation
- $10,000 in miscellaneous equipment.

This comes to $3.72E+04. In addition, the emergency procedures are estimated to require 4 man-months for formal development and implementation. This comes to $3.63E+04, for a total of $7.36E+04. The value/impact ratio is then estimated at 2.04 man-rem/$1000. Costs could thus increase by a factor of 2 to $155,000 and still give a figure on the order of 1 man-rem/$1000.

Allow Initiation of the EFW System Via Low SG Level Indication

As with the previous sequence, the automatic actuation of the EFW system would prevent the progression of the scenario to SG dryout. Allowing actuation on low SG levels would be the logical modification. Again, ORNL studies indicate that 1E "startup range" level signals for EFW valve control are already in place.

The costs associated with this fix will not be estimated directly, but again risk reduction could likely approach 90 percent of 7.73 man-rem/py, or 2.09E+02 man-rem over 30 years. This is in addition to the 659 man-rem risk reduction for the ISC hand power dryout scenario. This equates to $209,000 for this scenario alone to stay above the 1 man-rem/$1000 figure of merit. If the benefit of risk reduction from EFW automatic initiation in the previous dryout

scenario for ICS hand power failure is included, this figure could go to $659,000 + $209,000 = $868,000, or approximately $1,000,000 and still approach the 1 man-rem/$1000 figure of merit. ORNL estimates costs at approximately $100,000 giving a value/impact ratio of 8.68E+02 man-rem/$100,000 = 8.7.

4.4 SUMMARY OF VALUE/IMPACT

The proposed modifications to the B&W plant and the associated reduction in risk, estimated cost and value/impact are summarized in Table 4.3. Note that this is not meant to present an all-inclusive list of the failure modes and possible fixes resulting from the ORNL examination of control system failures in the Oconee B&W plant. The ORNL study is quite extensive, with a number of failure mechanisms identified that may, in fact, contribute to the potential safety concerns associated with A-47. However, the scenarios examined here are thought to represent those failures of greatest safety concern, and the modifications summarized below address those scenarios directly.

The implementation of monthly testing, with an additional FTPX relay added to allow online testing of the entire circuit, certainly appears cost-effective. More reliable high-level configurations such as a 2-out-of-4 also appear cost-effective. Implementation of such hardware changes after going to monthly testing would reduce the value/impact ratios by approximately a factor of 10, making such changes slightly less viable for the B&W Oconee plant, but still giving value/impact ratios only slightly below 1 man-rem/$1,000. Modifications to prevent ICS power failures appear to be very cost-effective.

TABLE 4.3. Summary of the Value/Impact Analysis for the Oconee B&W Plant

Proposed Fix	Scenario Affected	Estimated Cost, $1000	Estimated Risk Reduction (man-rem)	Value/Impact Ratio (man-rem/$1000)
Monthly Testing	Overfill & undetected high trip failure	293	4.53E+02	5.2
Monthly Testing Plus Parallel FTPX Relay	Same as above	200	1.05E+03	5.3
Feedwater Block Valve Trip Circuit		83	1.34E+03	16.2

TABLE 4.3. (Continued)

Proposed Fix	Scenario Affected	Estimated Cost, $1000	Estimated Risk Reduction (man-rem)	Value/Impact Ratio (man-rem/$1000)
Modified Trip Logic (See Note 1)				
1. 1-out-of-1, 1 FTPX with two spurious trips in 30 years		624	4.53E+02	0.73
2. 1-out-of-2, 1 FTPX with two spurious trips in 30 years		612	8.99E+02	1.47
3. 2-out-of-3, 1 FTPX		300	8.86E+02	3.0
4. 1-out-of-2, 2 FTPX with two spurious trips in 30 years		636.0	1.15E+03	1.8
5. 2-out-of-3, 1 FTPX per LT		312	1.15E+03	3.7
6. 2-out-of-4, 1 FTPX		600	9.07E+02	1.5
7. 2-out-of-4, 2 FTPX		612	1.17E+03	1.9
MFW Trip on Loss of ICS Hand Power	ICS Hand Power Failure with SG dryout	-	-	-
Higher Minimum MFW Setpoint		-	-	-
MFW Default to 50% output on 0 Voltage (see Note 2)		- 6.59E+05	- 6.59E+02	- 1.0
Annunciation of Auto Power Failure and Emergency Procedures	Auto Power Failure	7.36E+04	1.55E+02	2.04

TABLE 4.3. (Continued)

Proposed Fix	Scenario Affected	Estimated Cost, $1000	Estimated Risk Reduction (man-rem)	Value/Impact Ratio (man-rem/$1000)
EFW Initiation on Low SG Level (see Note 2)	ICS Power Failures	1.0E+05	8.68E+02	8.68

Note 1: Cost of any or all of above can be less than $659,000 and still give a value/impact ratio equal to or greater than 1 man-rem/$1000.

Note 2: Cost of implementing the EFW initiation function can be as high as $868,000 or approximately $1,000,000 per plant and still give a value/impact ratio on the order of 1 man-rem/$1000.

5.0 CONCLUSIONS FOR THE B&W OCONEE PWR

The results of the consideration of core-melt potential for control system failures in the Oconee B&W PWR are summarized in the following table. The subjective judgment of which sequences to analyze was made from an extensive review of control system failures and possible interactions identified by ORNL. This examination is thus not meant to represent an exhaustive study of all failure modes and the associated risk in the Oconee plant, but does represent a risk study of those failures thought to present the most serious safety concerns to the A-47 program at this time.

TABLE 5.1. Summary of ORNL and PNL Estimates of Accident Initiator Frequencies, Core-melt Frequencies, and Public Risk for the B&W Oconee PWR

	Accident Initiating Frequency Best Estimate[a] (/py)	PNL Core-Melt Frequency Best Estimate (/py)	PNL Public Risk Best Estimate (man-rem/py)
Sequence Initiator			
Overfill & High Trip Failure	0.006		
T2 Transient Shutdown		6.88E-08	1.86E-01
MSLB		6.27E-08	1.71E-01
SGTR		9.45E-06	4.54E+01
		9.58E-06	4.58E+01
ICS Hand Power Failure with SG Dryout	0.009	9.00E-06	2.44E+01
ICS Auto Power Failure	0.009		
SG Dryout		2.70E-06	7.31E+00
T2 Transient Shutdown		0	0
MSLB		1.16E-09	3.14E-03
SGTR		8.77E-08	4.21E-01
		2.79E-06	7.73E+00
TOTAL		2.14E-05	7.79E+01

(a) ORNL estimates of initiating frequencies, including operator error.

The three scenarios examined involved several failures of control systems that might progress to more severe failures, primarily centering on the feedwater systems. The potential for overfill of the steam generators progressing to spillover into the steam lines was identified by ORNL, along with scenarios for feedwater failures combining with operator failure to reestablish flow, thus progressing to core-melt.

Typical regulatory requirements for plant recovery give no credit for possible operator actions in the first 10 minutes of an accident. However, as the A-47 issue deals with control systems routinely under operator control, the interaction of the operator with failure diagnosis and recovery is an appropriate consideration. Several of the recommendations for reducing the potential for control system failures leading to more serious actions center on factors which aid in operator awareness, diagnosis, and correct response. As a result, several recommendations for A-47 might well be integrated with operator training and transient response programs.

Steam Generator Overfill

The steam generator overfill scenario examined deals with the potential in the Oconee plant for undetected failures in the high SG level MFW trip function. The associated risk was examined for progression to several scenarios: a transient shutdown with the power conversion system unavailable due to degrading conditions in the secondary side, overfill progressing to spillover and main steam line break (MSLB), and MSLB progressing to SGTR.

The resulting estimate of risk is given in Table 5.1. As can be seen, the contribution from progressing to SGTR is dominant for the above scenario. The assumption was made that the steam lines would have a 50 percent probability of failure given spillover of water into the steam lines after reactor trip, and a 50 percent probability that the break would occur outside of the reactor building where water released from the break would not be available for collection in building sumps for recirculation. The ability to isolate the affected steam generator can play an important role in recovery from a SGTR, but the Oconee plant has no motor-operated MSIVs. A category 2 type release was then assumed for public risk, involving an early core-melt with failure of the containment sprays which is consistent with exhaustion of recirculation inventories.

The potential for MSLB given spillover and the likely break location thus play an important role in the potential for progressing to core-melt given SGTR. Break location, however, is not as important in Oconee due to the lack of MSIVs as compared to the H.B. Robinson plant examined earlier for the A-47 program. The Oconee plant, however, is apparently not representative of all B&W plants.

The design modifications proposed to reduce the frequency of this scenario focus on the potential for undetected failures in the high-level MFW trip circuit. This failure probability was assumed to be fairly high by ORNL due to

an annual inspection frequency. Reducing this to a monthly basis was assumed to reduce the failure potential proportionally. This testing would be possible for most components (i.e., comparative signal readings from transmitters, etc.), however, the trip relays themselves are in series. The ORNL suggestion to add an additional FPTX relay to make the trip relay circuits associated with each generator parallel in configuration was then examined. This would make it possible to test the generator trip circuits alternately during operation.

The man-rem reduction associated with the monthly testing of this new trip circuit was estimated at 1050 man-rem over 30 years. The costs associated with the modification and testing were estimated at approximately $200,000, giving a value/impact ratio of 5.3 man-rem/$1000.

The addition of a feedwater block valve isolation on high SG water level appears to be effective in terminating any overfill scenario, providing another valve closure. If driven by an independent level transmitter signal, such as from the start-up range transmitters, a block valve trip would effectively eliminate the scenario. If costs for such a modification are under approximately $250,000, the value/impact ratio would also be more favorable than modifications for testing.

Note that no modifications to a 2-out-of-3 or 2-out-of-4 trip logic were postulated by ORNL. Given the different control function of the level transmitters and high trip in the B&W design, the analysis of such modifications is highly uncertain at this time. A simple reliability comparison indicates that a 2-out-of-3 or 2-out-of-4 logic could give similar value/impact ratios as compared to the increased testing discussed above. Implementation of monthly testing first would, however, reduce the risk for any subsequent hardware charges, and hence reduce the latter's value/impact ratio. Less uncertainty is also associated at this time with the reliability of monthly testing versus gains through equipment modifications. As a result, the monthly testing is thought to represent the better choice at this time.

Loss of ICS Hand Power

The loss of the ICS hand power circuit was found to present the potential for steam generator dryout if the operator were to fail to reestablish feedwater flow in 30 minutes or HPI flow in 60 minutes following loss of this power supply. Several modifications were developed which could potentially reduce the frequency of automatically progressing to dryout. These included MFW trip on loss of hand power which would initiate EFW flow, a higher minimum runback setpoint on the MFW to prevent the zero MFW flow in this case, and rewiring the loss-of-voltage signal to the MFW pump controller to represent a 50 percent setting as is apparently used in other B&W plants.

The potential risk reduction was estimated at 659 man-rem over 30 years. No costs for the above modifications were estimated. It was pointed out, however, that the above modifications were thought to be easily under this amount, giving value/impact ratios in excess of 1 man-rem/$1000.

Loss of Auto Power

The loss of auto power was initially thought to leave the plant in an unstable equilibrium, allowing the operator time to manually control the reactor before the development of an instability and subsequent trip. Oconee personnel indicated that this is how they would respond to such a failure. However, ORNL studies of the failure indicated that no annunciators are associated directly with the HI circuit which serves the majority of feedwater components. Nor were any emergency procedures found. As a result, an event tree assuming eventual reactor trip without prior operator awareness of the failure was assumed. The operator would then be required to reestablish feedwater flow as with the above scenario.

Annunciated power failure and proper emergency procedures in lowering operator error were estimated to provide a 155 man-rem risk reduction over 30 years. The costs for implementing such modifications were estimated to be minimal, giving a value/impact ratio of 2 man-rem/$1000.

Initiation of EFW on Low Level

The final modification examined was the automatic initiation of EFW on low-level signals from the steam generator level transmitters. This modification would effectively eliminate the two scenarios above that require operator action to reestablish feedwater before dryout of the generator occurs.

The modification does not appear to degrade or in any way jeopardize the current operating mode of the EFW, providing as it does only an additional initiation signal. However, this modification is not allowed by current NRC practices, involving as it does a cross-tie between a safety and non-safety grade system. Implementation would thus likely require a full safety upgrade of the level transmitting equipment if this philosophy were maintained.

Note that ORNL did not make an estimate of the upper bound for the initiating frequency of the scenarios identified. As a result, PNL has simply carried through an estimate of core-melt and public risk based on "best engineering estimates."

This analysis compares to the overall core-melt frequency for the Oconee plant of 8.20E-05/py with a public risk of 207 man-rem (Kolb et al. 1981). The consideration of the overfill scenario leading to spillover and the dryout scenarios thus represent a significant fraction (26 percent) of this risk.

REFERENCES

Andrews, W. B., et al. 1983. Guidelines for Nuclear Power Plant Safety Issue Prioritization. NUREG/CR-2800, Pacific Northwest Laboratory, Richland, Washington.

Bickford, W. E. and A. S. Tabatabai. 1985a. Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor. PNL-5545, NUREG/CR-4387, Pacific Northwest Laboratory, Richland, Washington.

Bickford, W. E. and A. S. Tabatabai. 1985b. Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor. PNL-5545, NUREG/CR-4385, Pacific Northwest Laboratory, Richland, Washington.

Bruske, S. J., et al. 1985. Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor Main Report. NUREG/CR-4262, Idaho National Engineering Laboratory, E.G.& G. Idaho, Inc., Idaho Falls, Idaho.

Clark, F. H., et al. 1985. An Assessment of the Safety Implications of Control at the Oconee-1 Nuclear Plant. NUREG/CR-4047, Oak Ridge National Laboratory, Oak Ridge, Tennessee.

Electric Power Research Institute (EPRI). 1982. ATWS: Part 3, Frequency of Anticipated Transients. NP-2230, EPRI, Palo Alto, California.

Electric Power Research Institute (EPRI). 1984. A Probabilistic Risk Assessment of Oconee Unit 3 - Summary Report. NSAL-60, EPRI, Palo Alto, California.

Heaberlin, S.W., et al. 1983. A Handbook for Value-Impact Analysis. NUREG/CR-3568, PNL-4646, Pacific Northwest Laboratory, Richland, Washington.

Institute of Nuclear Power Operations (INPO). 1982. Review of NRC Report: Precursors to Potential Severe Core Damage Accidents: 1969-1979 - A Status Report NUREG/CR-2497. INPO 82-025, INPO, Atlanta, Georgia.

Kolb, et al. 1981. Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant. NUREG/CR-1659/2, SAND80-1897/2, Sandia National Laboratories, Albuquerque, New Mexico.

Lewis, S. R., et al. 1984. Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3. NSAC/60-54, Electric Power Research Institute, Palo Alto, California.

Minarick, J. W. and C. A. Kukielka. 1982. Precursors to Potential Severe Core Damage Accidents: 1969-1979. NUREG/CR-2497, Science Applications, Inc., Oak Ridge National Laboratory, Oak Ridge, Tennessee.

Nuclear Regulatory Commission (NRC). 1975. Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400, NUREG-75/014, U.S. NRC, Washington, D.C.

Nuclear Regulatory Commission (NRC). 1983. NRC Integrated Program for the Resolution of Unresolved Safety Issues A-3, A-4, and A-5 Regarding Steam Generator Tube Integrity. NUREG/-0844, U.S. NRC, Washington, D.C.

Nuclear Regulatory Commission (NRC). 1983a. Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission. NUREG/BR-0058, U.S. NRC, Washington, D.C.

Nuclear Regulatory Commission (NRC). 1983b. A Prioritization of Generic Safety Issues. NUREG-0933, U.S. NRC, Washington, D.C.

Ransom, C. B., et al. 1985. Effects of Control System Failure on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor. NUREG/CR-4326, Idaho National Engineering Laboratory, E.G.& G Idaho, Inc., Idaho Falls, Idaho.

Stevens, D. L., et al. 1983. VISA-A Computer Code for Predicting the Probability of Reactor Pressure Vessel Failure. NUREG/CR-3384, PNL-4774, Pacific Northwest Laboratory, Richland, Washington.

NUREG/CR-4386
PNL-5544
RG, R1, R4

DISTRIBUTION

No. of
Copies

OFFSITE

U.S. Nuclear Regulatory Commission
Division of Technical Information
and Document Control
7920 Norfolk Avenue
Bethesda, MD 20014

Division of Risk Analysis and
Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

A. J. DiPalo (20)
M. L. Ernst
F. P. Gillespie
J. A. Murphy
P. W. Baranowsky
J. C. Belote
J. C. Melaro
G. R. Burdick

Division of Safety Technology
Office of Nuclear Reactor Regulations
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

A. J. Szukiewicz (10)
N. Anderson
K. Kniel
W. Minners

D. L. Basdekas
Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Oak Ridge National Laboratory
Oak Ridge, TN 37831

F. H. Clark
S. J. Ball

No. of
Copies

ONSITE

32 Pacific Northwest Laboratory

W. B. Andrews
W. E. Bickford (10)
A. S. Tabatabai (10)
M. F. Mullen
R. E. Rhoads
R. J. Sorenson
J. L. Braitman
Publishing Coordination (2)
Technical Information (5)

NRC FORM 335 (2-64) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG/CR-4386
PNL-5544

2. TITLE AND SUBTITLE
Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: October
YEAR: 1985

5. AUTHOR(S)
W.E. Bickford, A.S. Tabatabai

6. DATE REPORT ISSUED
MONTH: December
YEAR: 1985

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Pacific Northwest Laboratory
Richland, WA 99352

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER
B2386

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

11a. TYPE OF REPORT
Technical

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

Pacific Northwest Laboratory (PNL) performed probabilistic risk analyses aimed at developing estimates of core-melt frequency and public risk associated with control system failures in a Babcock and Wilcox pressurized water reactor, and value/impact analyses of proposed systems modifications. These analyses were based on the results of failure modes and effects analyses previously performed at the Oak Ridge National Laboratory (ORNL). The control system failure modes that were identified by ORNL and analyzed by PNL fall into three main scenarios: 1) overfill of the steam generators progressing to spillover into the steam lines, 2) ICS hand power failure progressing to steam generator dryout, and 3) ICS automatic power failure progressing to steam generator failure. For each of these modes, failure sequences were postulated. The results of PNL's probabilistic analysis of failure progression to core damage and value/impact analyses of possible resolutions to prevent the occurrence of these failures are presented in this report.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS
probabilistic risk analyses
control system failure modes

b. IDENTIFIERS/OPEN ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

FREQUENCIES AT A BABCOCK AND WILCOX PRESSURIZED WATER REACTOR